CISCO
Collaboration

CISCO The bridge to possible

Webex Meetings Security

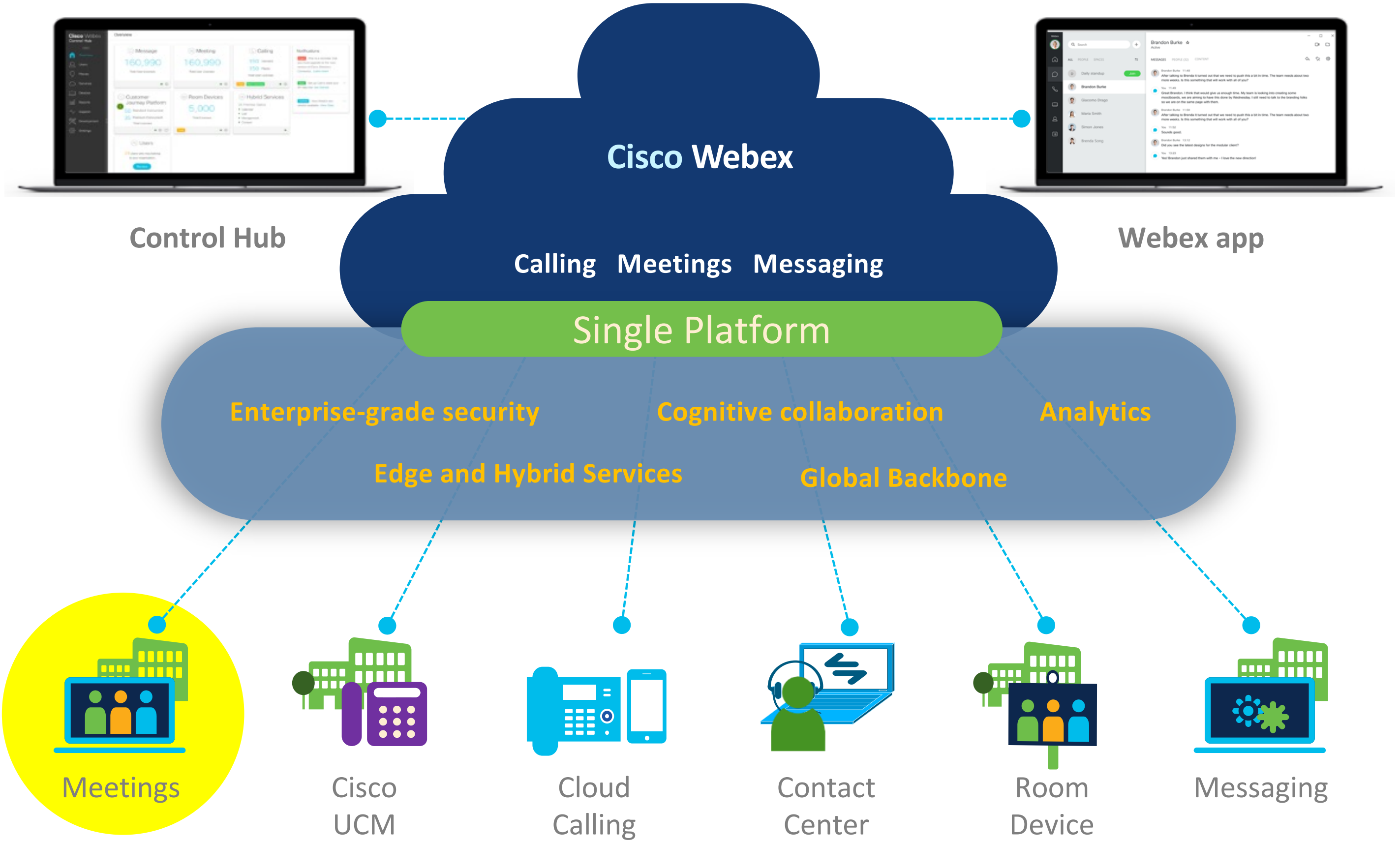
Jaroslav Martan
jmartan@cisco.com
Sep 21st 2021

High Level Agenda

- Controlling access to Webex Meetings
- New End to End Encryption for Webex Meetings
- End to End Identity for Webex Meetings
- Summary and Roadmap

Cisco’s Commitment to Security

Single Webex Platform – Multiple cloud services



Control Hub

Webex app

Cisco Webex

Calling Meetings Messaging

Single Platform

Enterprise-grade security

Cognitive collaboration

Analytics

Edge and Hybrid Services

Global Backbone

Meetings

Cisco UCM

Cloud Calling

Contact Center

Room Device

Messaging

Cisco Webex Meetings and your data

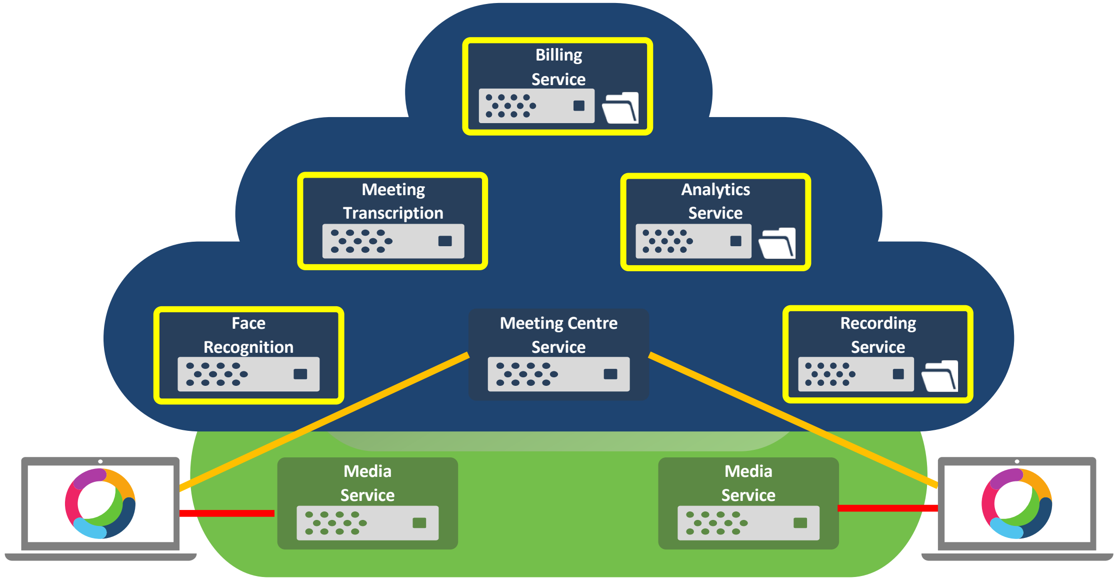
Webex Meetings are ephemeral, and by default we do not persist your meeting content

If you chose to record or transcribe your Webex meeting – the content will be securely stored in your region
Recordings and transcripts are encrypted using AES-256-GCM

Cisco also stores Billing information
and Meeting Analytics information

See Privacy data sheet for details

Intelligent cloud services :
- Face recognition
- Noise detection and suppression -
Meeting transcription
Are Cisco Webex owned technologies.



https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf

Controlling access to Webex Meetings

Controlling access to Webex Meetings

Agenda

- Authenticating Users and Devices
- Securing Access to Webex Meetings
  - Planned changes to User Classifications
- Webex Meeting User Interface
  - Planned changes to Lobby and Roster List user details for E2E Encrypted Meetings

Webex Meetings : Authenticating Users and Devices

Device Type	Sign In/ Authentication Methods	
Webex app	Webex Identity	Enterprise IdP (SSO)
Webex Web app	Webex Identity	Enterprise IdP (SSO)
Cloud registered Webex Room devices	Webex Identity (Device Onboarding + Machine Account)	
PSTN user	Webex Identity (CLID + Audio PIN)	
SIP device	Enterprise domain (CA signed certificate on Expressway-E/ SIP Edge device (SBC) – Mutual TLS to Webex Cloud	

Benefits of User and Device Sign In/Authentication for Webex Meetings :

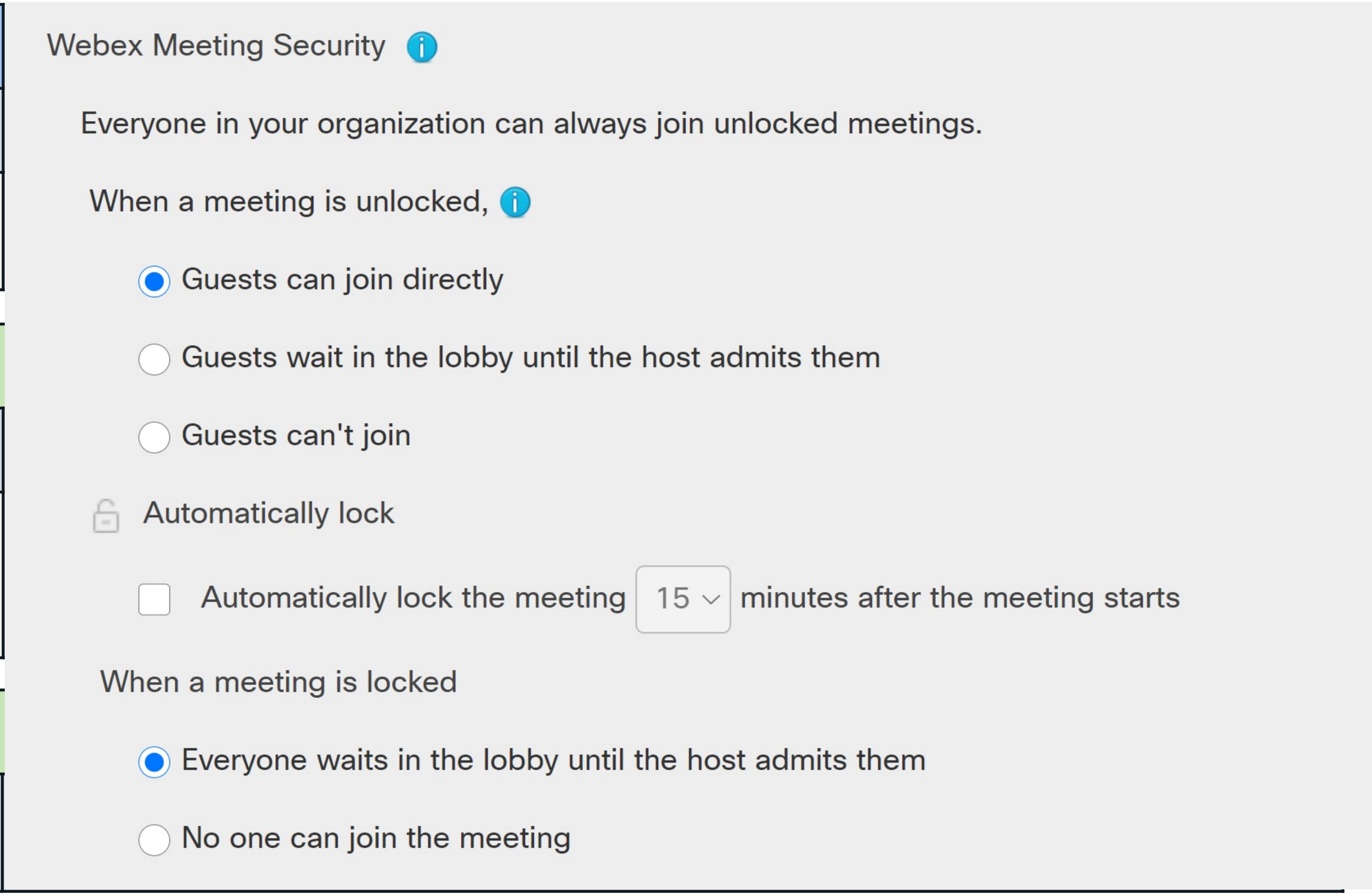
- **Secure access to meetings for Users in your Webex organization**
- **Simplifies access to your Webex Meetings :**
  - Authenticated users can join unlocked meetings directly -
  Unauthenticated user meeting access can be controlled

Securing Access to Webex Meetings
Current User Types (Control Hub Admin)

User Types
Signed In Users
Guest Users

Unlocked Meeting Access options
Signed In Users
Guest Users

Locked Meeting Access options
All Users



Webex Meeting Security

Everyone in your organization can always join unlocked meetings.

When a meeting is unlocked,

- ● Guests can join directly
- ○ Guests wait in the lobby until the host admits them
- ○ Guests can't join

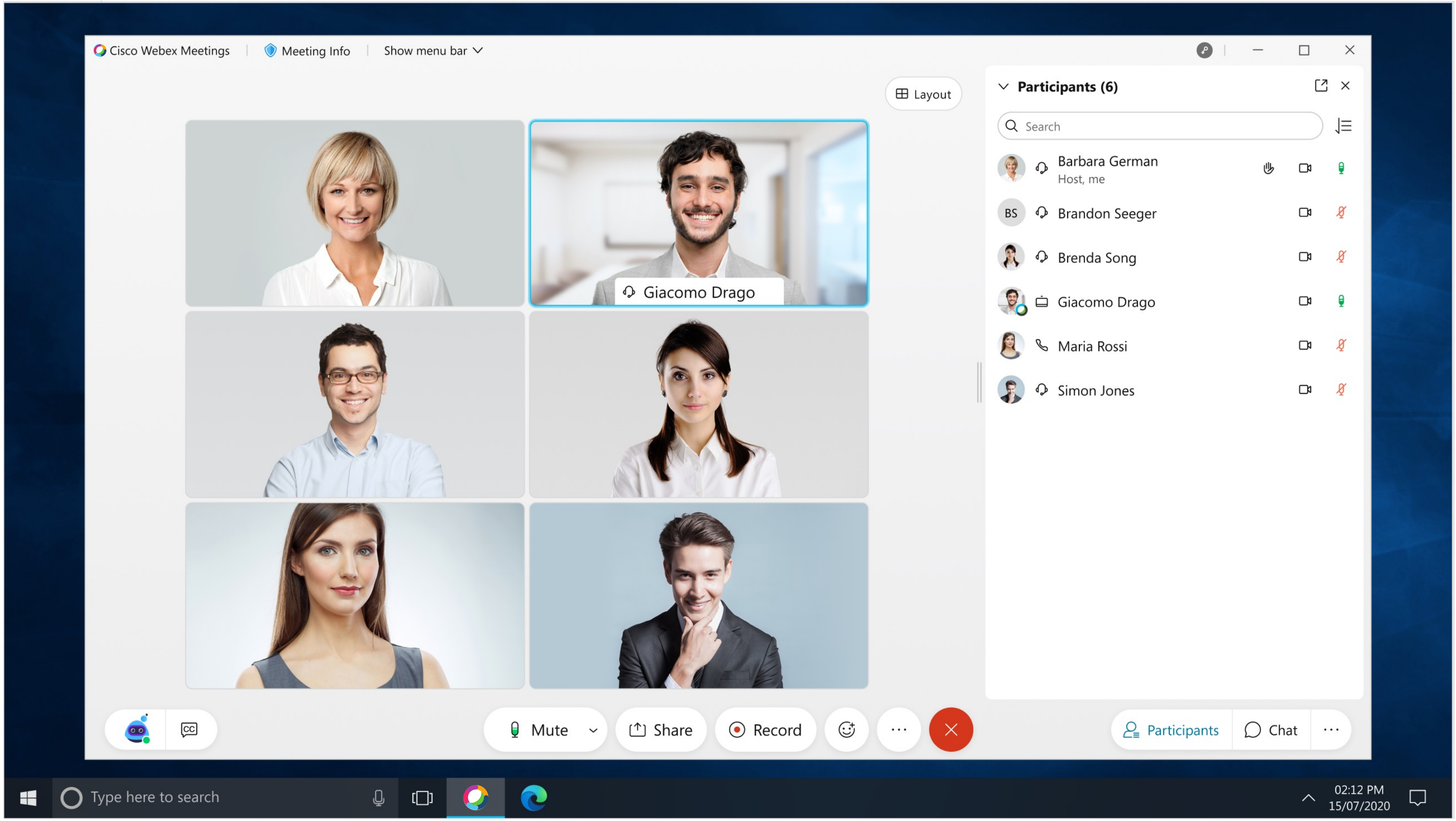
Automatically lock

- □ Automatically lock the meeting 15 minutes after the meeting starts

When a meeting is locked

- ● Everyone waits in the lobby until the host admits them
- ○ No one can join the meeting

Current Webex Meetings UX
Meeting Roster User Details

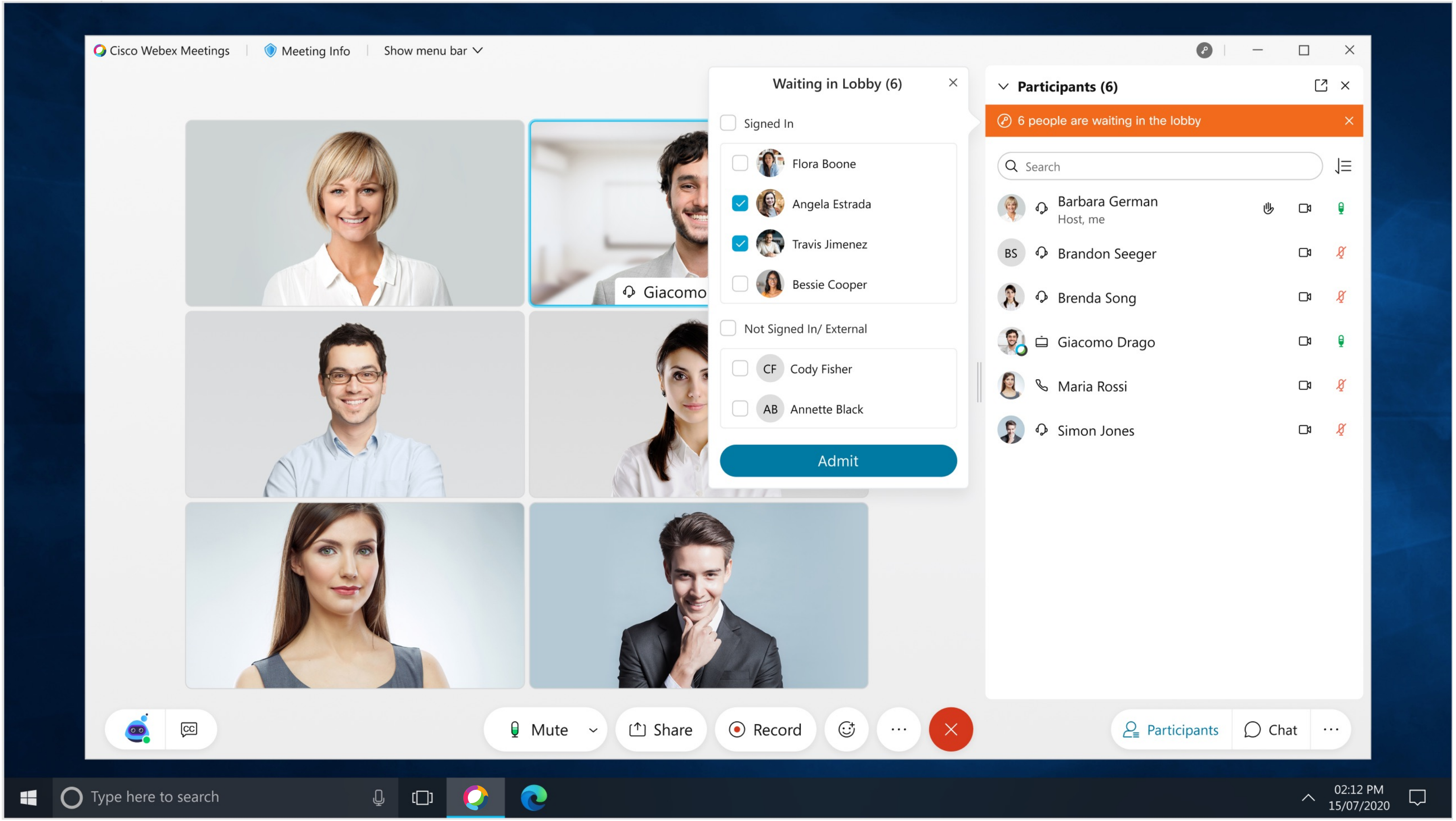


Participants (6)

Search

- Barbara German — Host, me
- Brandon Seeger
- Brenda Song
- Giacomo Drago
- Maria Rossi
- Simon Jones

Current Webex Meetings UX
Meeting Lobby User Categories



Cisco Webex Meetings | Meeting Info | Show menu bar

Waiting in Lobby (6)

□ Signed In

- □ Flora Boone
- ☑ Angela Estrada
- ☑ Travis Jimenez
- □ Bessie Cooper

□ Not Signed In/ External

- □ CF Cody Fisher
- □ AB Annette Black

Admit

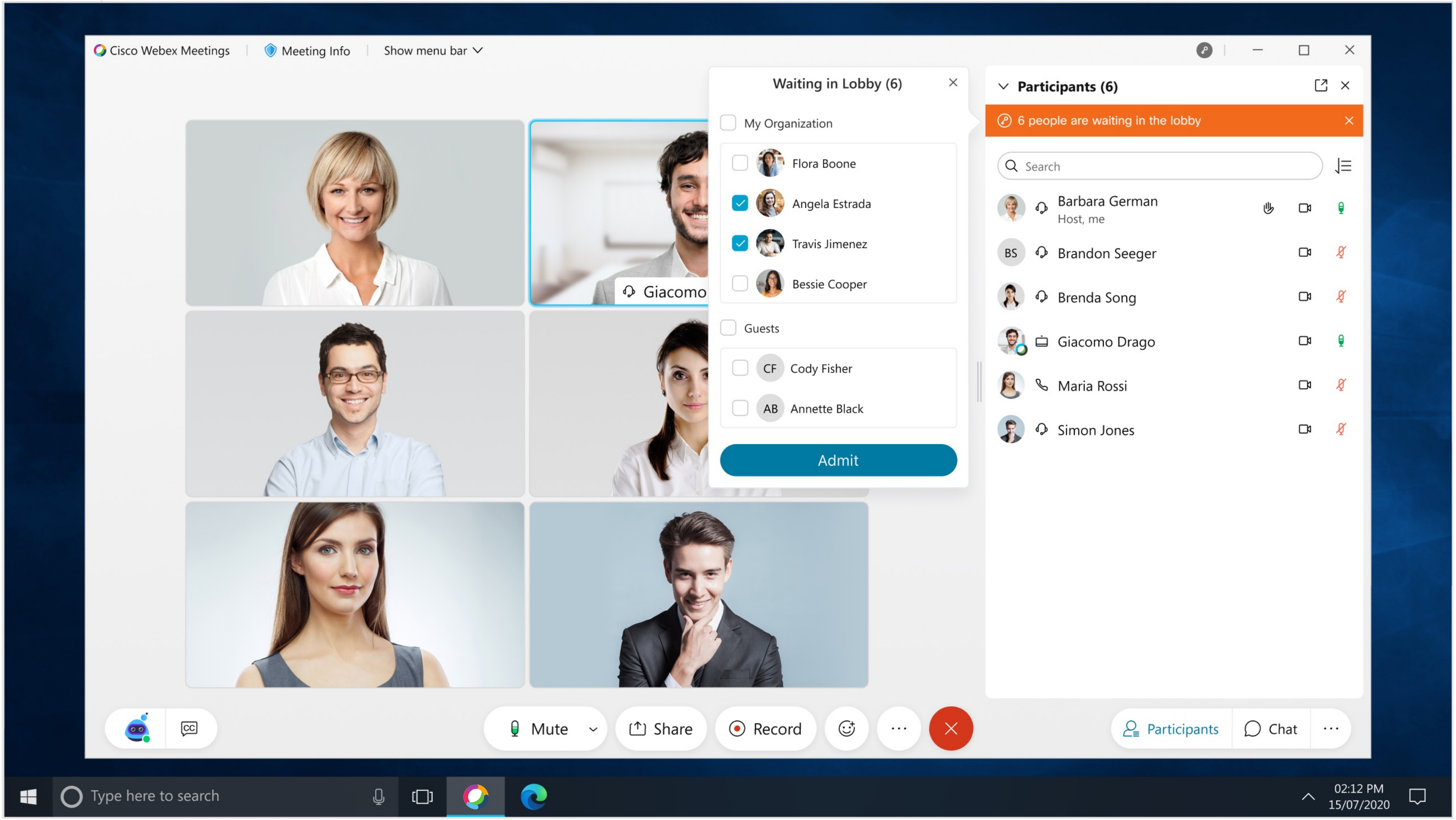
Participants (6)

6 people are waiting in the lobby

Search

- Barbara German, Host, me
- BS Brandon Seeger
- Brenda Song
- Giacomo Drago
- Maria Rossi
- Simon Jones

Standard Encrypted Webex Meetings UX
Planned change to Webex Meeting Lobby User Categories



Waiting in Lobby (6)

□ My Organization

- □ Flora Boone
- ☑ Angela Estrada
- ☑ Travis Jimenez
- □ Bessie Cooper

□ Guests

- □ CF Cody Fisher
- □ AB Annette Black

Admit

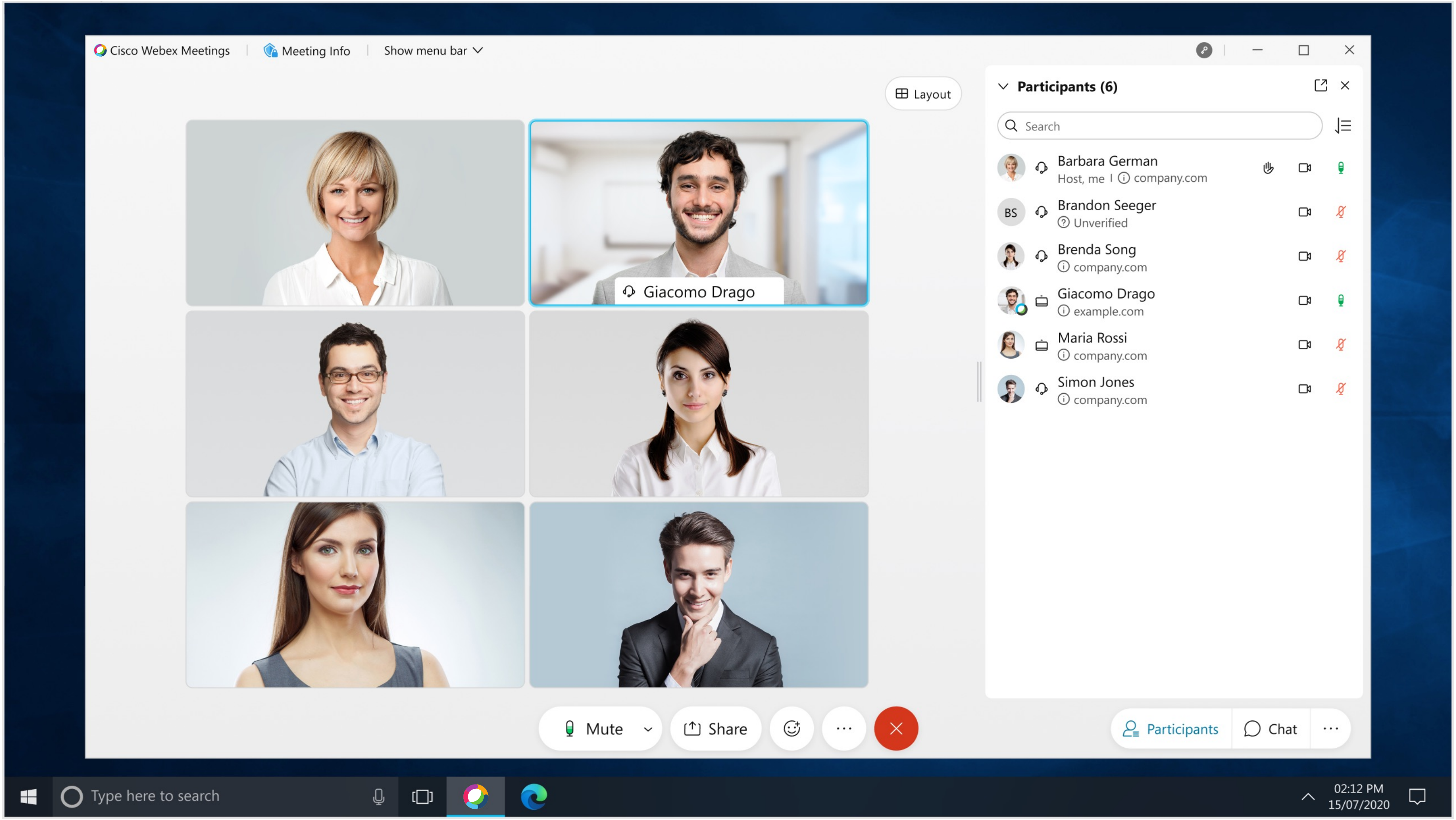
Participants (6)

6 people are waiting in the lobby

Search

- Barbara German, Host, me
- BS Brandon Seeger
- Brenda Song
- Giacomo Drago
- Maria Rossi
- Simon Jones

Zero Trust Security for Webex Meetings
E2E Encrypted Meeting Roster List - New User Details



Participants (6)

Search

Barbara German
Host, me | ⓘ company.com

BS Brandon Seeger
ⓘ Unverified

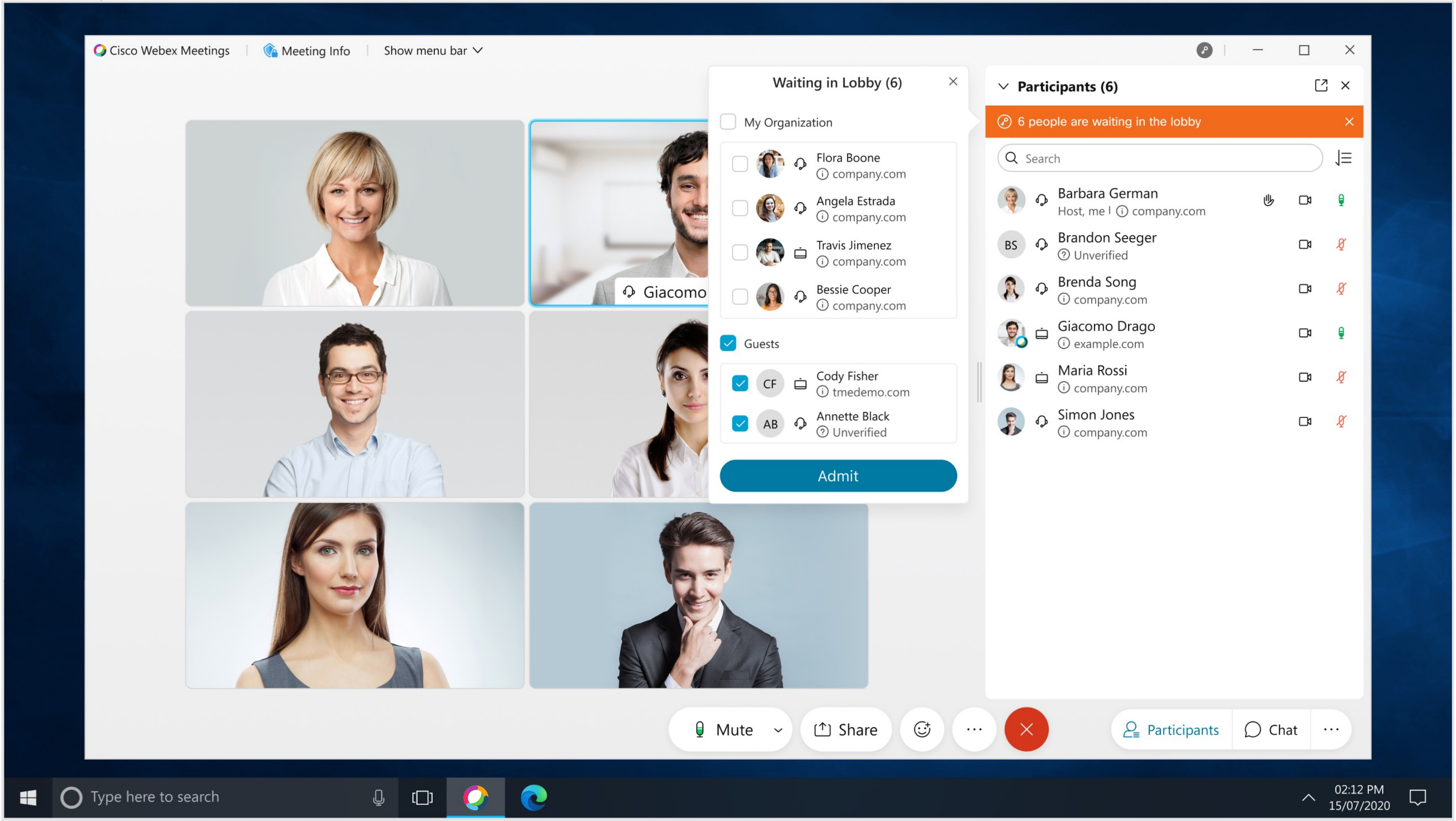
Brenda Song
ⓘ company.com

Giacomo Drago
ⓘ example.com

Maria Rossi
ⓘ company.com

Simon Jones
ⓘ company.com

Zero Trust Security for Webex Meetings
E2E Encrypted Meeting Lobby - New User Details



Waiting in Lobby (6)

□ My Organization

- □ Flora Boone – company.com
- □ Angela Estrada – company.com
- □ Travis Jimenez – company.com
- □ Bessie Cooper – company.com

☑ Guests

- ☑ CF Cody Fisher – tmedemo.com
- ☑ AB Annette Black – Unverified

Admit

Participants (6)

6 people are waiting in the lobby

Search

- Barbara German – Host, me | company.com
- BS Brandon Seeger – Unverified
- Brenda Song – company.com
- Giacomo Drago – example.com
- Maria Rossi – company.com
- Simon Jones – company.com

End to End Encryption

What is End to End Encryption ?

https://en.wikipedia.org/wiki/End-to-end_encryption

“**End-to-end encryption** (**E2EE**) *is a system of communication where only the communicating users can read the messages. In principle, it prevents potential*

There are many definitions of End to End Encryption…. But in simple layman’s terms….

End to End Encryption is where your service provider does not have your encryption key and cannot decrypt your content

End-to-end encryption: The encryption of information at its origin and decryption at its intended destination without any intermediate decryption.

High Level Agenda

End to End Encryption

Question:
How do you know that your Meetings Provider does not have your meeting encryption key ?

Answer:

If you never exchange the actual meeting encryption key, and your provider cannot intercept your signalling without your knowledge

Webex Meetings End to End Encryption

Detailed Agenda

- Encryption for Webex Meetings today
- Zero Trust Security :
  - E2E Encryption and E2E Identity for Meetings
- Zero Trust Security : E2E Encrypted Meetings
  - MLS key packages and certificates
  - Webex Meetings – New User Experience
  - MLS operation – meeting participant join and leave
  - S-Frame Encryption
  - Meeting Security Codes

Encryption for Webex Meetings today

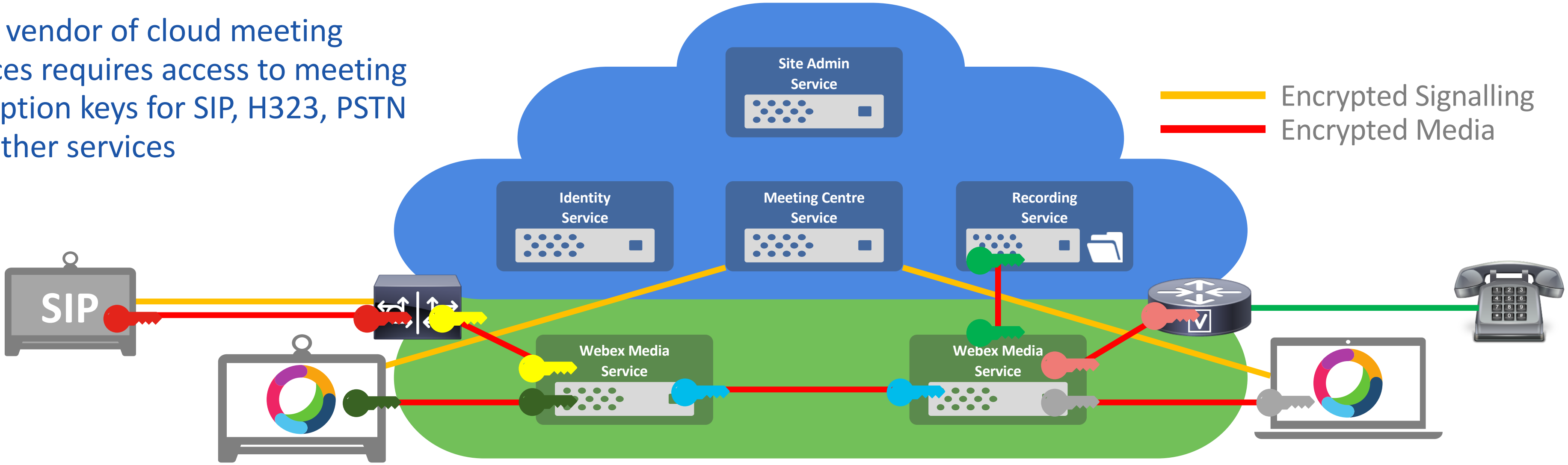
- Standard Encrypted Meetings
– E2E Encrypted Meetings

Encryption for standard Webex Meetings

With standard Webex Meetings, all signalling and media in the Webex cloud is encrypted
Webex apps and devices use encrypted signalling and encrypted media
SIP devices can encrypt signalling and media, PSTN audio is encrypted by the Webex cloud

With standard Webex Meetings, the cloud needs to access to encryption keys to decrypt SRTP media from SIP devices, PSTN gateways and for other services such as recording

Every vendor of cloud meeting services requires access to meeting encryption keys for SIP, H323, PSTN and other services

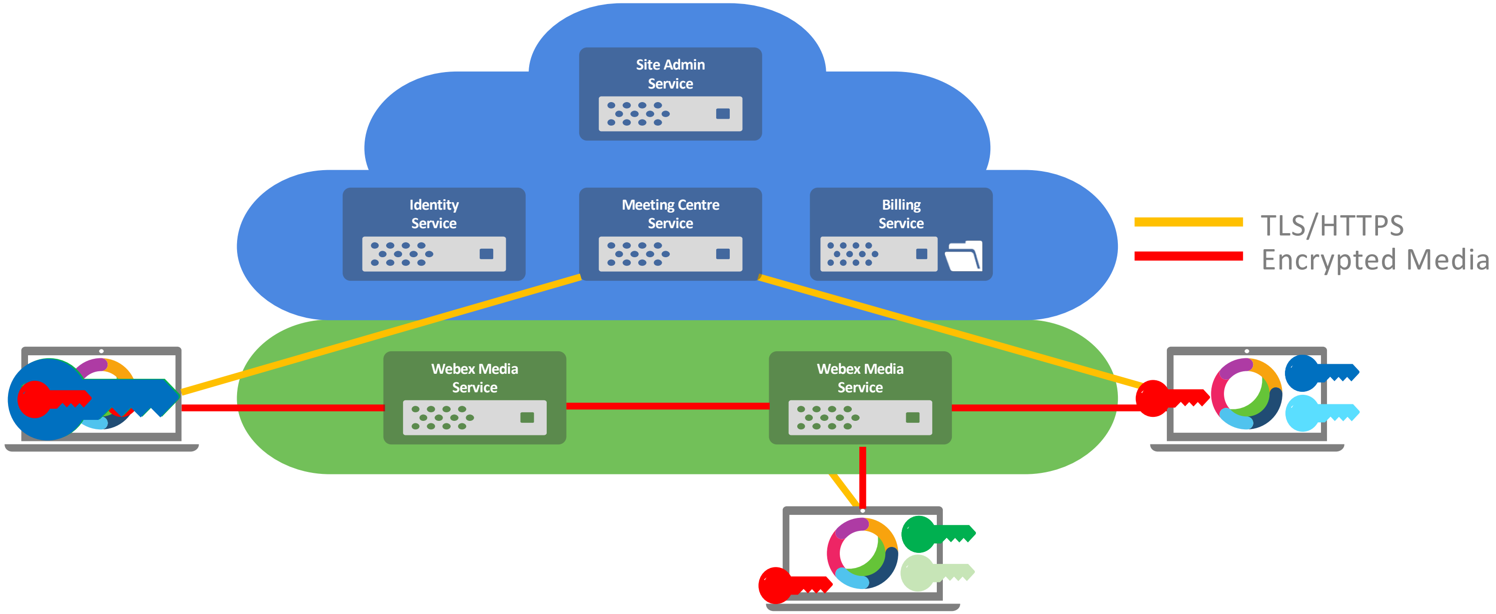


Confidential End-to-End Encrypted Webex Meetings

With E2E encrypted Meetings, the Webex cloud does not have access your meeting encryption key

The meeting encryption key is generated by the meeting host's Webex app

The meeting host encrypts the meeting key with participant's public and securely returns it over TLS



Cisco introduced E2E Encryption for Webex Meetings in 2008

https://help.webex.com/en-us/WBX44739/What-Does-End-to-End-Encryption-Do

Zero Trust Security for Webex Meetings

New
End to End Encryption & End to End Identity

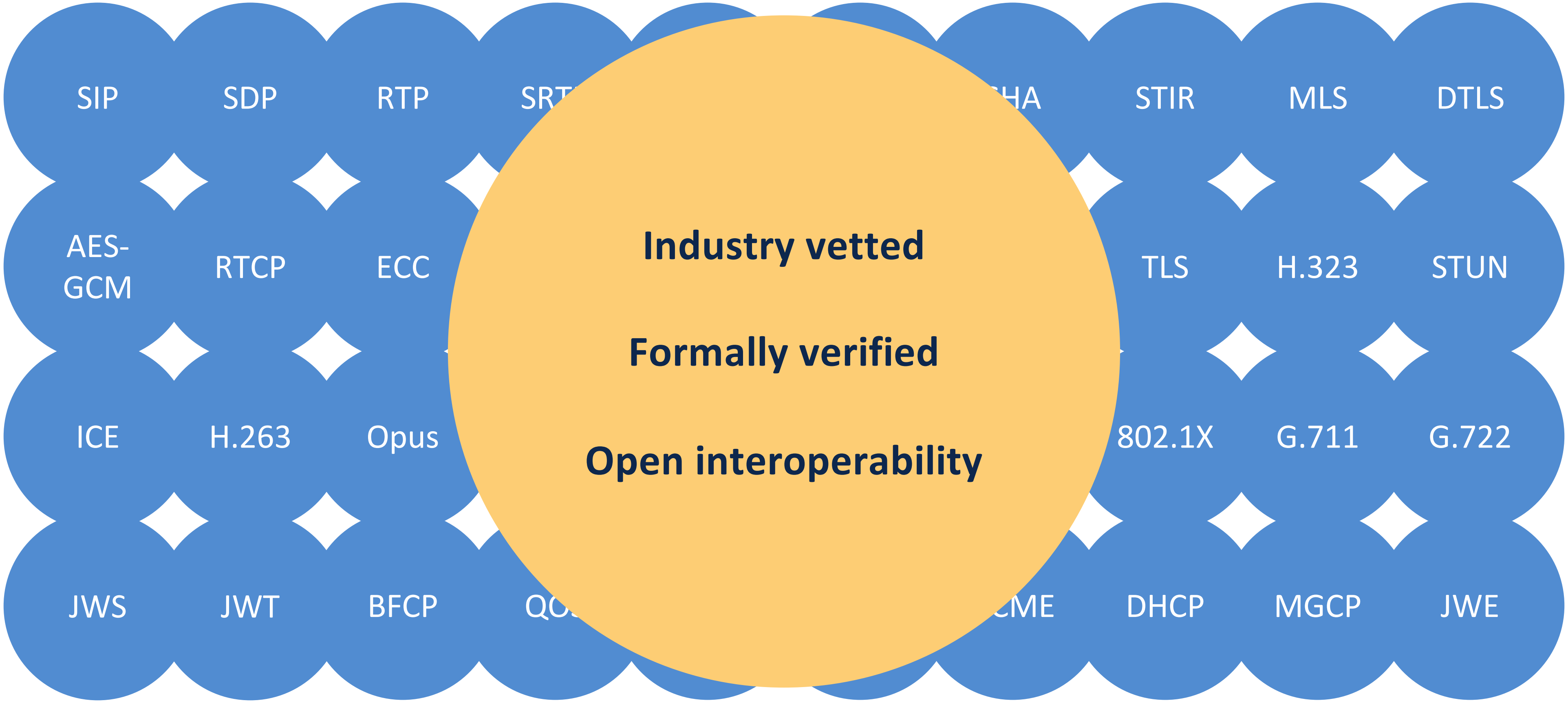
Zero-Trust Security :
Strengthening and extending E2E Encryption for Webex Meetings

Standards

Identity

Devices

Cisco’s engagement in standards-based innovation



SIP SDP RTP SRT HA STIR MLS DTLS

AES-GCM RTCP ECC TLS H.323 STUN

ICE H.263 Opus 802.1X G.711 G.722

JWS JWT BFCP QO CME DHCP MGCP JWE

Industry vetted

Formally verified

Open interoperability

New Standards for E2E Encrypted Webex Meetings

	Today	Zero Trust Security adds....
Identity	SSO (SAML, OpenID)	Automated Certificate Management Environment (ACME) Open Source!
Key Exchange	SDES / DTLS	Messaging Layer Security (MLS) Open Source!
Media Encryption	SRTP Open Source!	Secure Frames (SFrame) Open Source!

New Standards for E2E Encrypted Webex Meetings

Messaging Layer Security (MLS)

Developed as a security layer for E2E encrypting group messaging. Repurposed for Webex Meetings E2E encryption.

Certificates are used by MLS to identify meeting participants and as part of the MLS E2E encryption key generation process

https://tools.ietf.org/html/draft-ietf-mls-architecture-05
https://tools.ietf.org/html/draft-ietf-mls-protocol-11

Secure Frames (SFrame)

Secure Media Frames provides an extra layer of authenticated encryption for media.

The media frame is encrypted before being placed into individual SRTP payloads

SFrame uses MLS to provide the encryption keys that each meeting participant needs

https://tools.ietf.org/html/draft-omara-sframe
https://tools.ietf.org/html/draft-barnes-sframe-mls-00

Automated Certificate Management Environment (ACME)

The ACME protocol is used to generate user and device identity certificates. ACME automatically handles Certificate Signing Requests sent to Certificate Authorities

Device Cert. name validation via public DNS server name check

Username validation via SAML assertion from a federated IdP

https://tools.ietf.org/html/rfc8555
https://tools.ietf.org/html/draft-biggs-acme-sso-00

Webex Meetings E2E Encryption Implementations Feature Comparison

	Webex E2E Encryption (Today)	Webex E2E Encryption with Zero Trust Security
Based on standards track protocols	No	Yes
Encryption key traverses the cloud ?	Yes (Encrypted and sent over TLS)	No – Only meta data sent over TLS
Personal Meeting Rooms	No	Yes
Join Before Host	No	Yes
Lobby	No	Yes
Webex Web app	No	Planned
Video Device support	No (SRTP: Requires Webex key access)	Yes – Webex cloud registered devices
SIP devices	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
PSTN	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
Network Based Recording	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
Transcripts, Speech Recognition	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
Live streaming	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)

End to End Encryption from all meetings service providers share a common limitation in that SRTP based apps and devices cannot be supported - As this gives your provider access to the meeting encryption key

Rolling Out Zero Trust Security based E2E Encrypted Meetings

Requires no administrator or end user changes :

1) Cloud registered Webex Room devices will be upgraded to support E2E Encryption
2) The Webex app will be upgraded to support both forms of E2E encryption
3) Cluster by cluster enablement of Zero Trust E2E Encryption in the Webex cloud
4) When the cloud migration is completed, old E2E Encryption will be removed from the Webex app

MLS requires that all apps and devices have identity certificates

In this first phase, with End to End Encryption only, for zero touch roll-out :
The Webex CA will generate and distribute identity certificates to Webex apps and Webex Room devices

Zero Trust Security for Webex Meetings

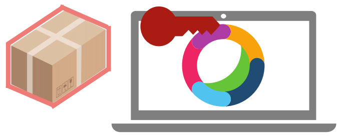
New
End to End Encryption

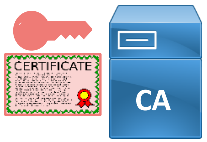
MLS for E2E Encrypted Webex Meetings

Messaging Layer Security (MLS)

Developed as a security layer for E2E encrypting group messaging. Repurposed for Webex Meetings E2E encryption.

Identity Certificates are used by MLS (in MLS key packages) to identify meeting participants and as part of the MLS E2E encryption key generation process
https://tools.ietf.org/html/draft-ietf-mls-architecture-05
https://tools.ietf.org/html/draft-ietf-mls-protocol-11



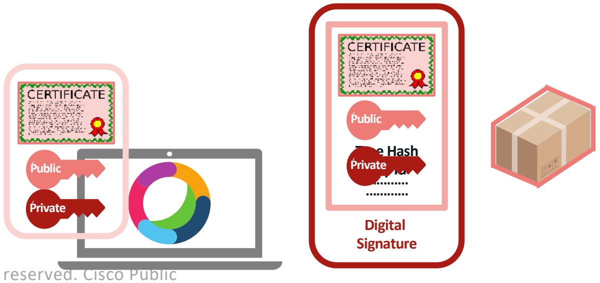


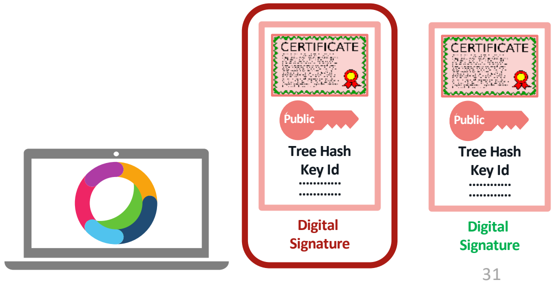
MLS uses "key packages" to identify users and to generate new meeting encryption keys as participants join and leave the meeting

Each MLS key package contains :

- The meeting participant's Identity Certificate
- A tree hash value that represents the cryptographic group state and credentials of the group members (meeting participants)
- An identifier for the current version of the meeting encryption key

Each meeting participant signs their key package with their private key, so that other meeting participants can verify its authenticity



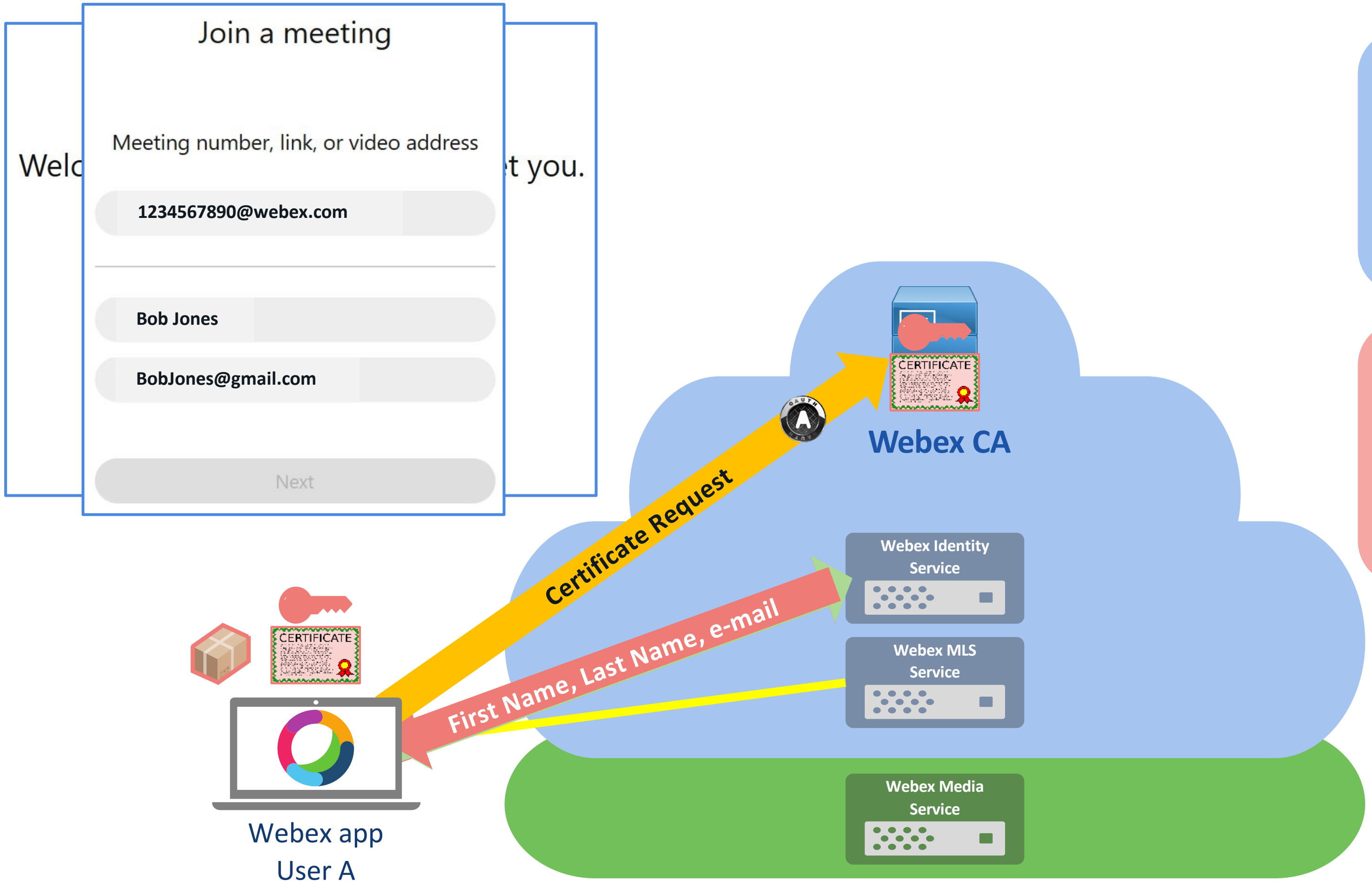


Zero Trust Security for Webex Meetings : Phase 1
New Webex E2E Encryption

User/Device Authentication and Identity Certificates

User/Device Type	Authentication	Certificate Authority	Lobby/Roster User status
Webex app	Not Signed In (Meeting Join without Sign In)	Webex CA	? **Unverified** (Hover on icon for CA and Cert details)
Webex app	Webex Identity service	Webex CA	ⓘ example.com (Hover on icon for CA and Cert details)
Webex app	Enterprise IdP (SSO)	Webex CA	ⓘ example.com (Hover on icon for CA and Cert details)
Webex Cloud registered Device	Machine Account	Webex CA	ⓘ example.com (Hover on icon for CA and Cert details)

Users who have Not Signed In : Webex CA Identity Certificates :



Welc … t you.

Join a meeting

Meeting number, link, or video address

1234567890@webex.com

Bob Jones

BobJones@gmail.com

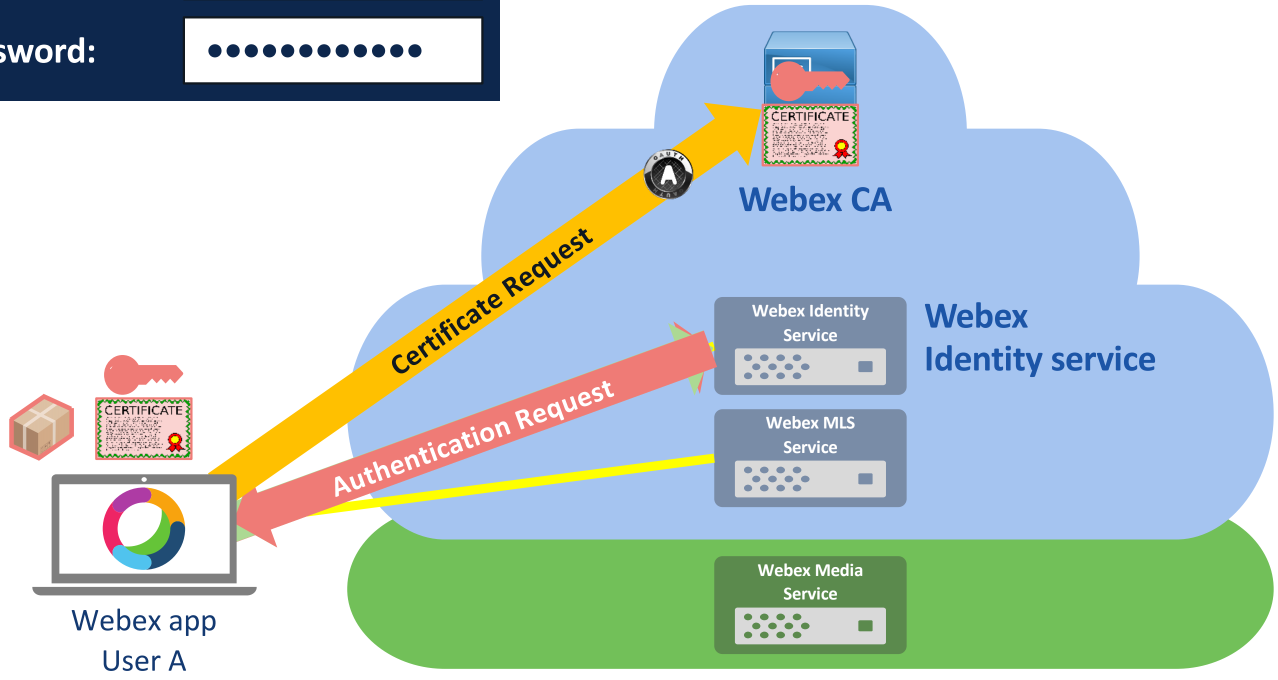
Users who have Not Signed In are assigned a temporary UUID and OAuth access token

Users who have Not Signed In are listed as **Unverified** in the Meeting Lobby and Roster List

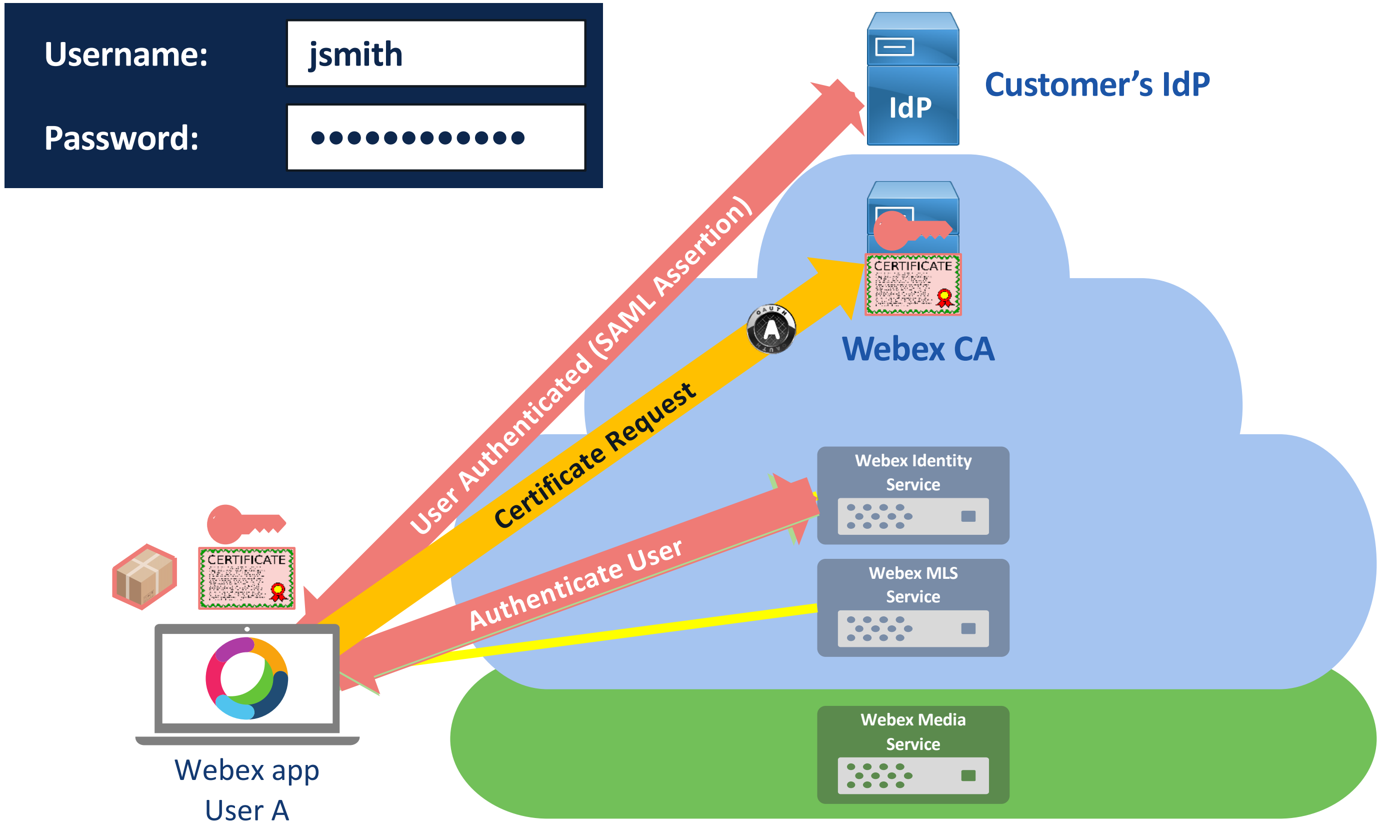
Meeting Host has Admit/Eject controls

Users Signing In with the Webex Identity service : Webex CA Identity certificates

Username:	jsmith
Password:	●●●●●●●●●●●●

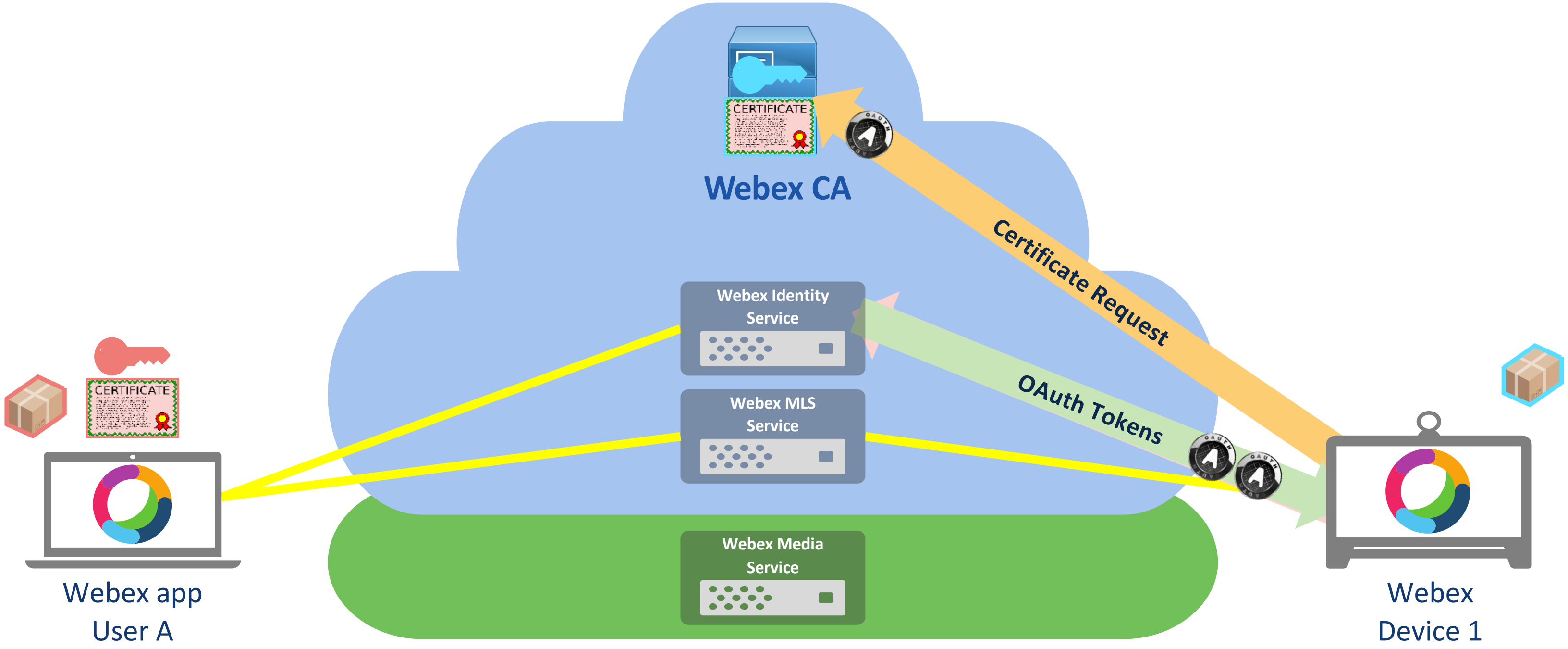


SSO Users - Signing In with their Enterprise IdP : Webex CA Identity certificates



Webex cloud registered Devices
(Machine account authentication with Webex Identity service)

Webex CA Identity certificates



Zero Trust Security for Webex Meetings

New

End to End Encryption
User Experience

Zero Trust Security for Webex Meetings
New Meeting Security icons : Encrypted/ E2E Encrypted

Encrypted Meeting :

Webex app, Webex Room devices, SIP devices, PSTN

Network based : Recording, Transcription, Speech Recognition, Closed Captions, Webex Assistant etc

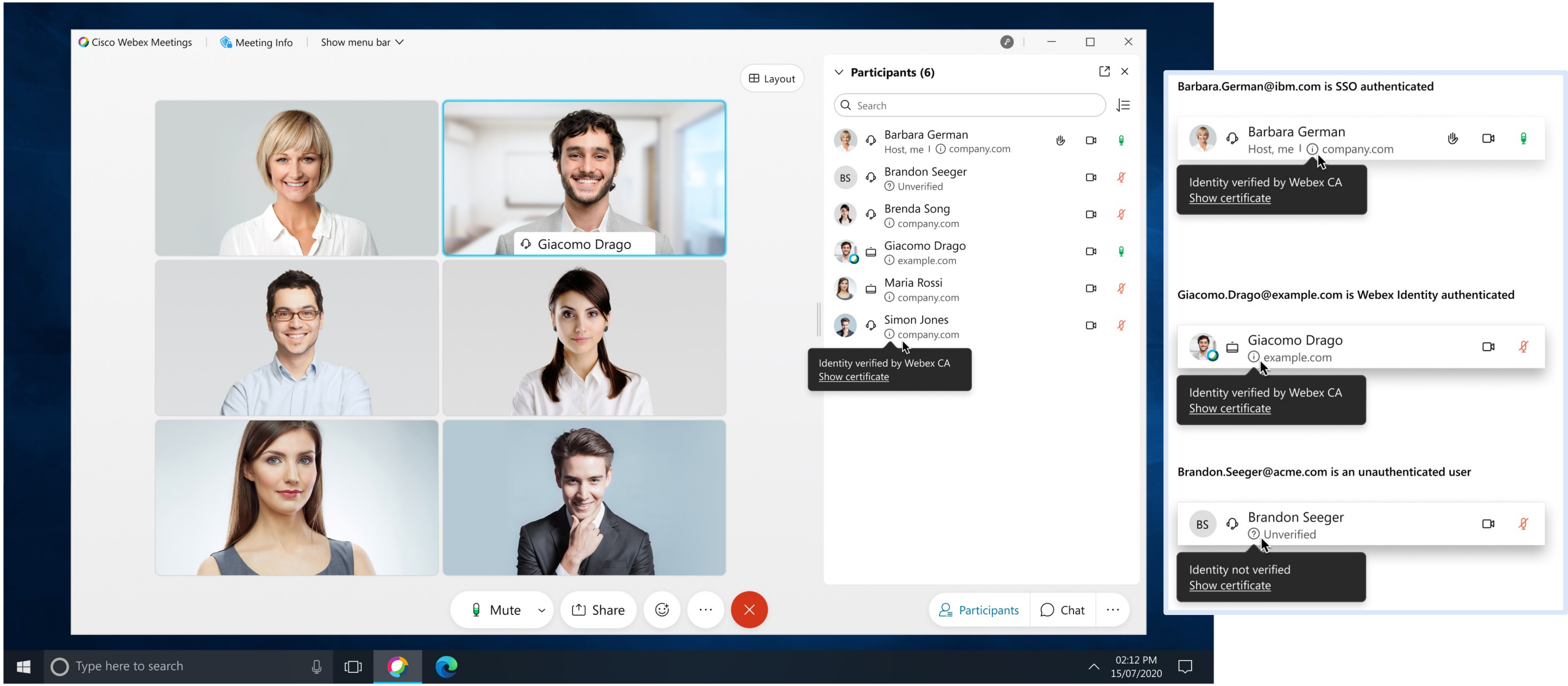
End to End Encrypted Meeting :

Webex app, Cloud registered Webex Room devices only

No SIP devices or PSTN users

No Network Services

Zero Trust Security for Webex Meetings
E2E Encrypted Meeting Roster List - New User Details



Participants (6)

Search

Barbara German
Host, me | ⓘ company.com

BS Brandon Seeger
? Unverified

Brenda Song
ⓘ company.com

Giacomo Drago
ⓘ example.com

Maria Rossi
ⓘ company.com

Simon Jones
ⓘ company.com

Identity verified by Webex CA
Show certificate

Barbara.German@ibm.com is SSO authenticated

Barbara German
Host, me | ⓘ company.com

Identity verified by Webex CA
Show certificate

Giacomo.Drago@example.com is Webex Identity authenticated

Giacomo Drago
ⓘ example.com

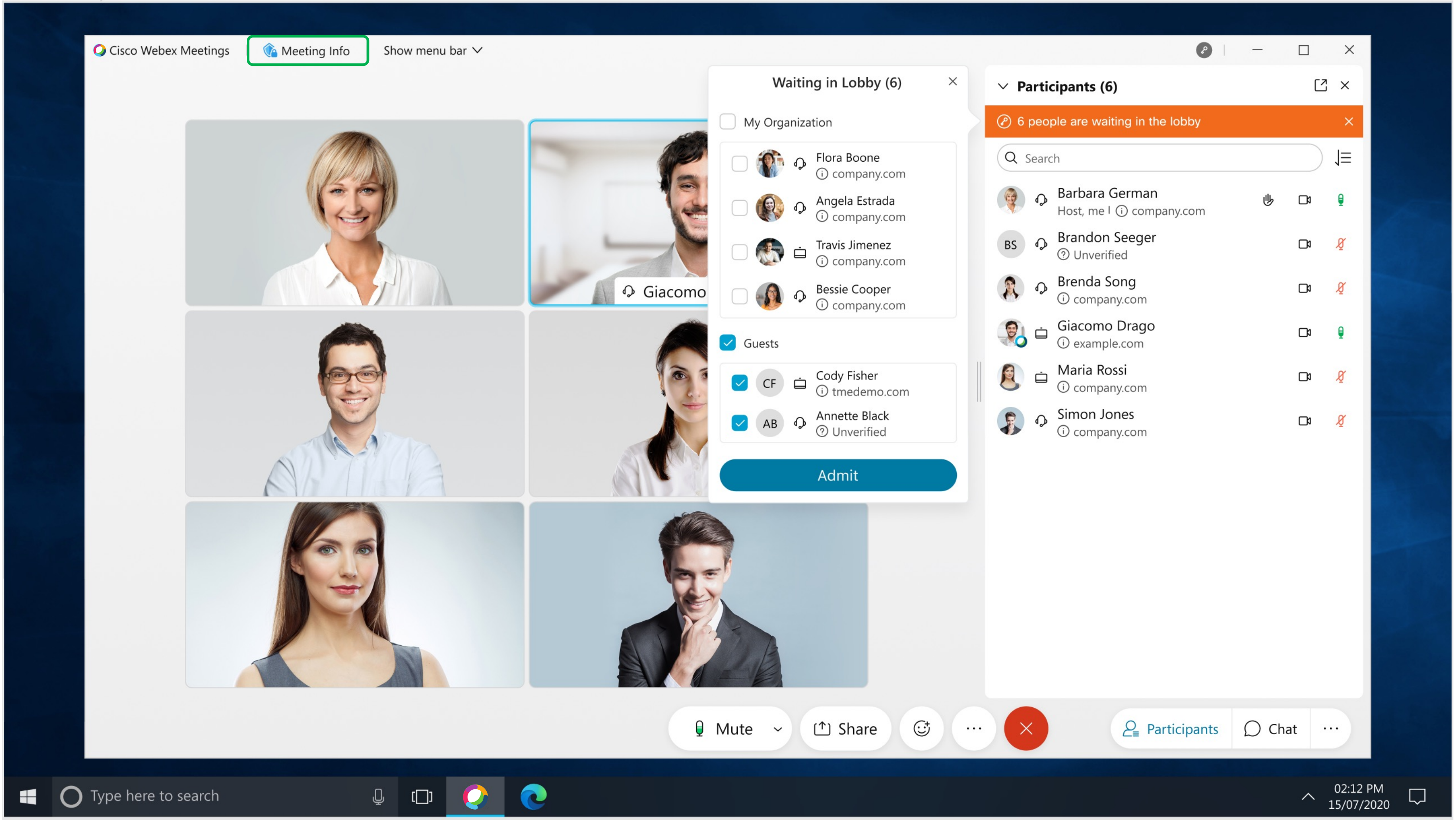
Identity verified by Webex CA
Show certificate

Brandon.Seeger@acme.com is an unauthenticated user

BS Brandon Seeger
? Unverified

Identity not verified
Show certificate

Zero Trust Security Webex Meetings
E2E Encrypted Meeting Lobby - New User Details



Waiting in Lobby (6)

□ My Organization

- □ Flora Boone — ⓘ company.com
- □ Angela Estrada — ⓘ company.com
- □ Travis Jimenez — ⓘ company.com
- □ Bessie Cooper — ⓘ company.com

☑ Guests

- ☑ CF Cody Fisher — ⓘ tmedemo.com
- ☑ AB Annette Black — ⓘ Unverified

Admit

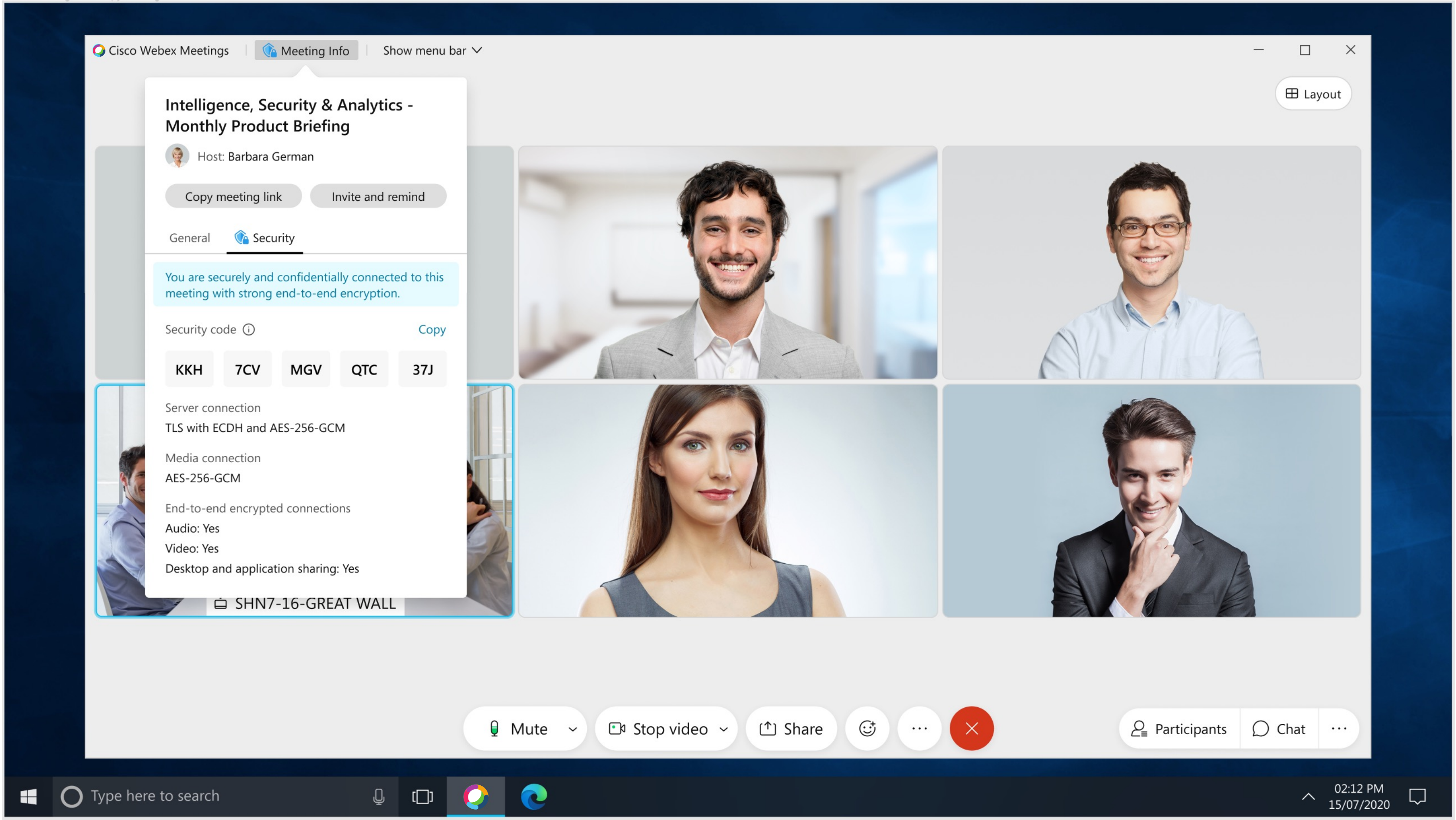
Participants (6)

6 people are waiting in the lobby

Search

Name	Details
Barbara German	Host, me ⓘ company.com
BS Brandon Seeger	ⓘ Unverified
Brenda Song	ⓘ company.com
Giacomo Drago	ⓘ example.com
Maria Rossi	ⓘ company.com
Simon Jones	ⓘ company.com

Zero Trust Security for Webex Meetings
E2E Encrypted Meeting Security Information



Intelligence, Security & Analytics - Monthly Product Briefing

Host: Barbara German

You are securely and confidentially connected to this meeting with strong end-to-end encryption.

Security code ⓘ

KKH 7CV MGV QTC 37J

Server connection
TLS with ECDH and AES-256-GCM

Media connection
AES-256-GCM

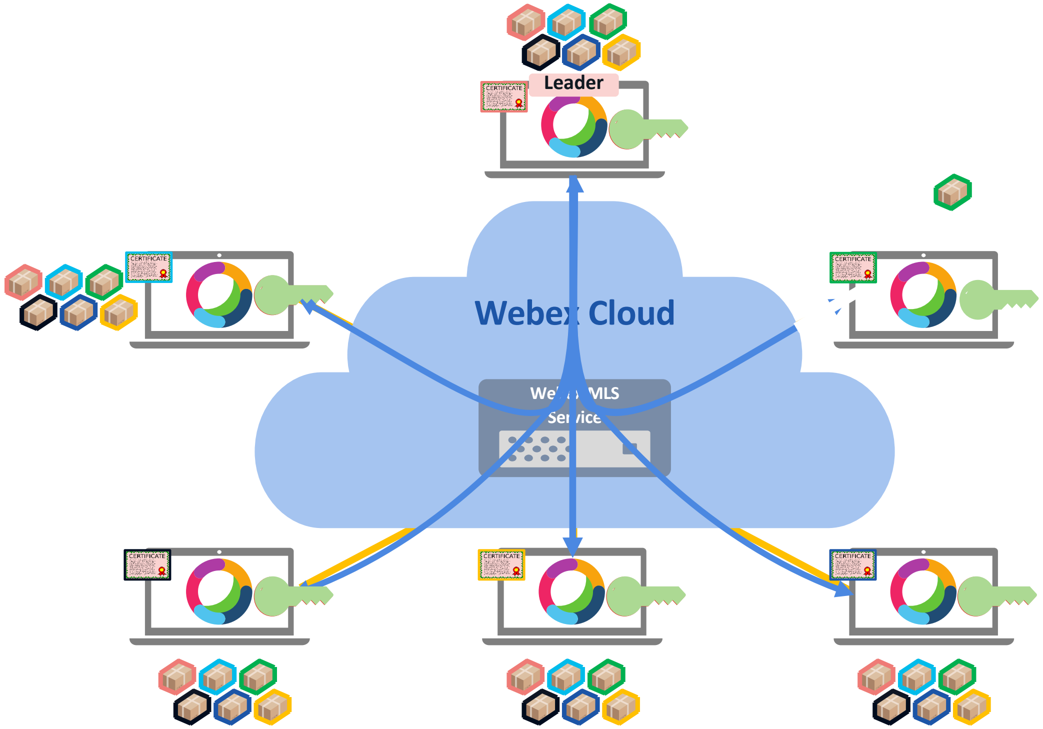
End-to-end encrypted connections
Audio: Yes
Video: Yes
Desktop and application sharing: Yes

Zero Trust Security for Webex Meetings

MLS and SFrame details

MLS Operation : Meeting Participant Join

MLS key package : contains the participant’s certificate and other meta data used for identity verification and meeting encryption key generation.



New meeting participants send their key package to the meeting leader (In MLS, the leader does not need to be the Meeting Host)

The meeting leader shares the new participant’s key package with the other participants.

The meeting leader shares the existing meeting participants’ key packages with the new participant.

All meeting participants generate a new meeting encryption key
(MLS uses timers to reduce key churn when large numbers of participants join the meeting in a short time interval)

A new meeting encryption key is created when participants join or leave the meeting

SFrame for E2E Encrypted Webex Meetings

Secure Frames
(SFrame)

Secure Media Frames provides an extra layer of authenticated encryption for media.

The whole media frame is encrypted before being placed into individual SRTP payloads

SFrame uses MLS to provide the encryption keys that each meeting participant needs

https://tools.ietf.org/html/draft-omara-sframe
https://tools.ietf.org/html/draft-barnes-sframe-mls-00

SFrame encryption cipher AES-256-GCM

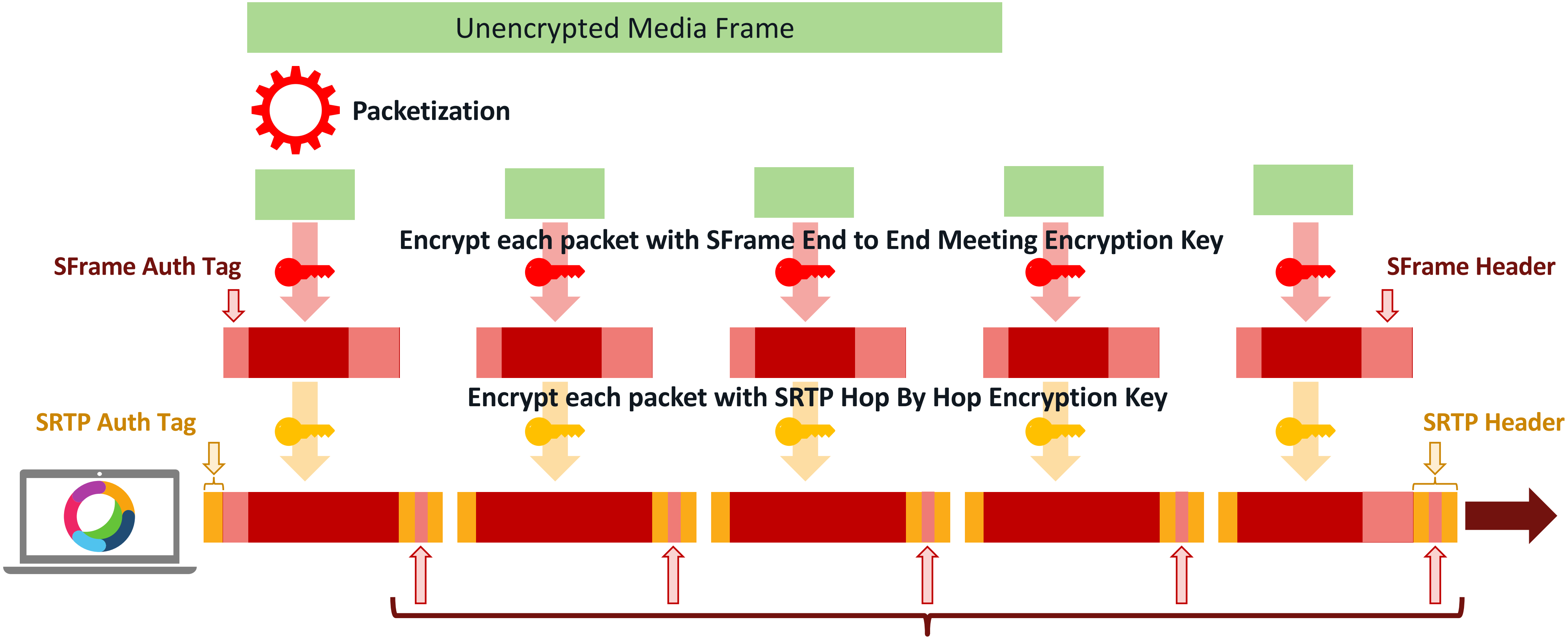
Double Encryption process

1) Unencrypted media frame
2) Packetize unencrypted media frame
3) Encrypt packets using SFrame E2E Meeting Encryption key
4) Encrypted SFrame packets -> Encrypted with SRTP keys
5) Media meta data moved to SRTP header extension (authenticated)

Encrypted SFrame format :
SFrame header – Frame counter (used for encryption IV) - Key Id
SFrame Encrypted Media
SFrame authentication tag

Authenticated SRTP header extension
Speaker volume indication (used by Webex media servers to switch media without decrypting SFrame content)

Secure Frames (SFrame)



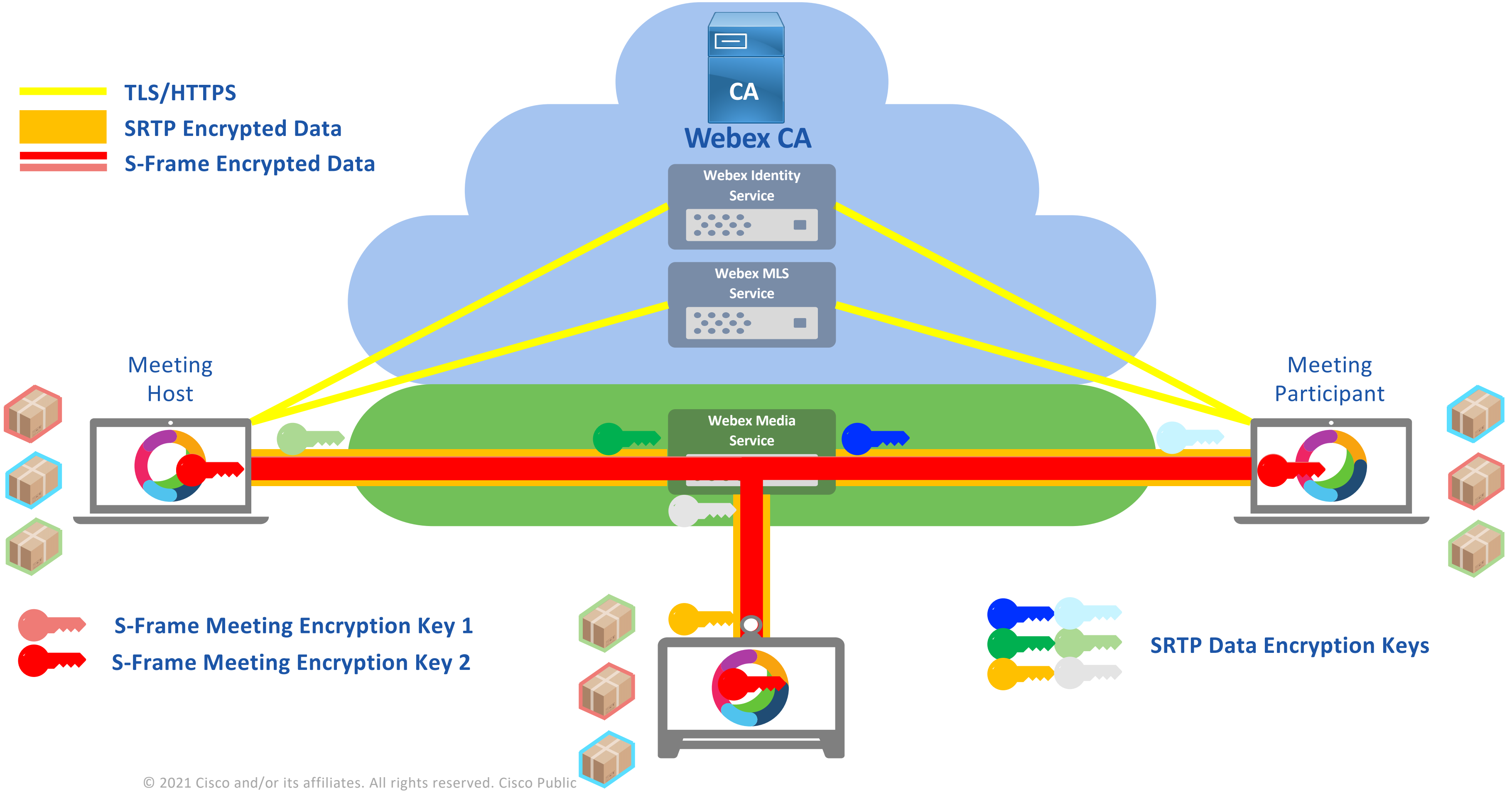
Unencrypted Media Frame
Packetization
Encrypt each packet with SFrame End to End Meeting Encryption Key
SFrame Auth Tag
SFrame Header
Encrypt each packet with SRTP Hop By Hop Encryption Key
SRTP Auth Tag
SRTP Header

SFrame media metadata (e.g. speaker volume) in RTP Header Extension
allows Webex media servers to switch data without needing to decrypt the SFrame content

Zero Trust Security for Webex Meetings

Combined MLS and SFrame operation

Zero Trust Security for Webex Meetings – E2E Encryption MLS and SFrame operation



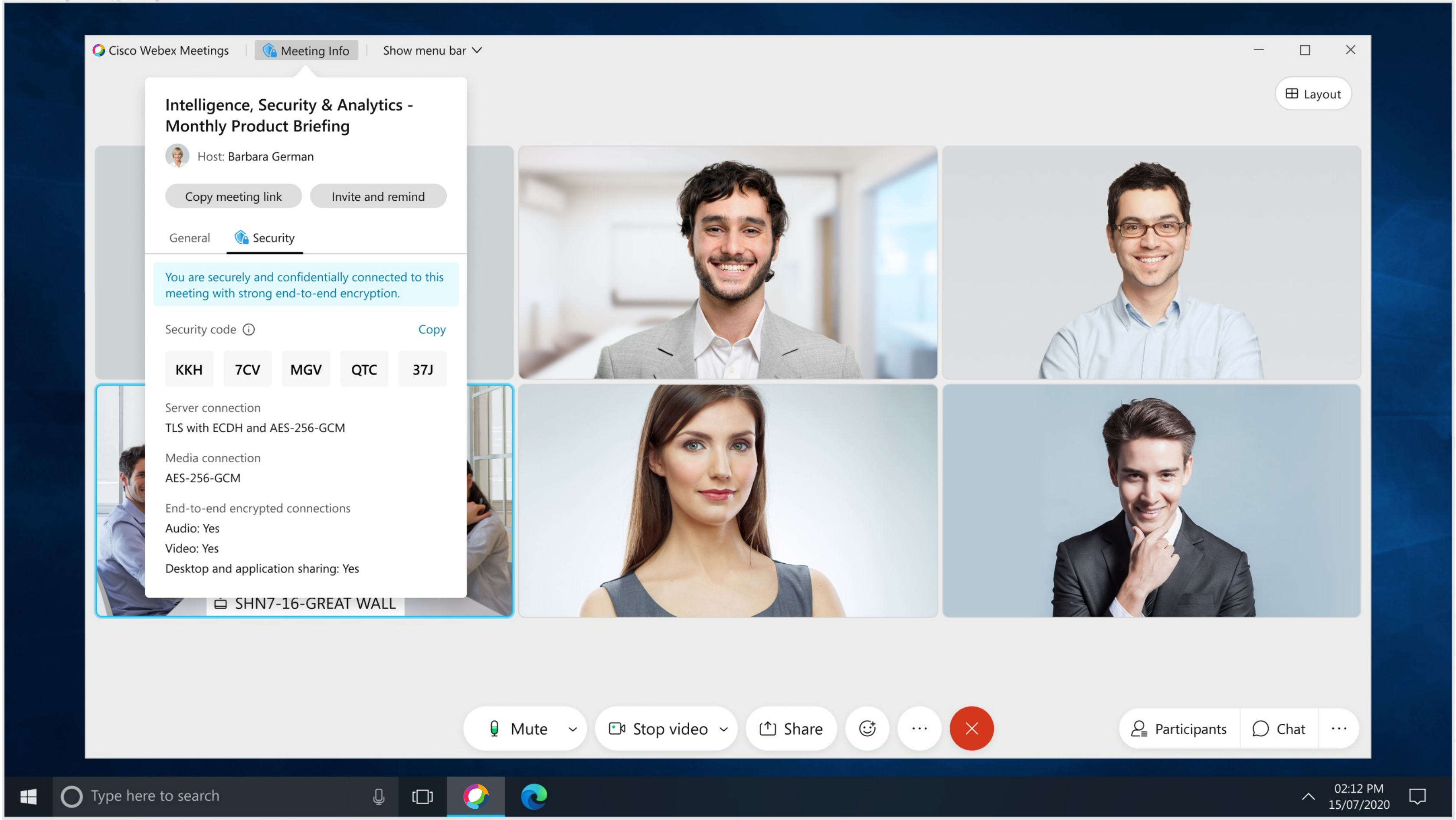
Zero Trust Security for Webex Meetings

New

End to End Encryption

Meeting Security Codes

Zero Trust Security for Webex Meetings
E2E Encrypted Meetings - Meeting Security Code



Intelligence, Security & Analytics - Monthly Product Briefing

Host: Barbara German

You are securely and confidentially connected to this meeting with strong end-to-end encryption.

Security code ⓘ

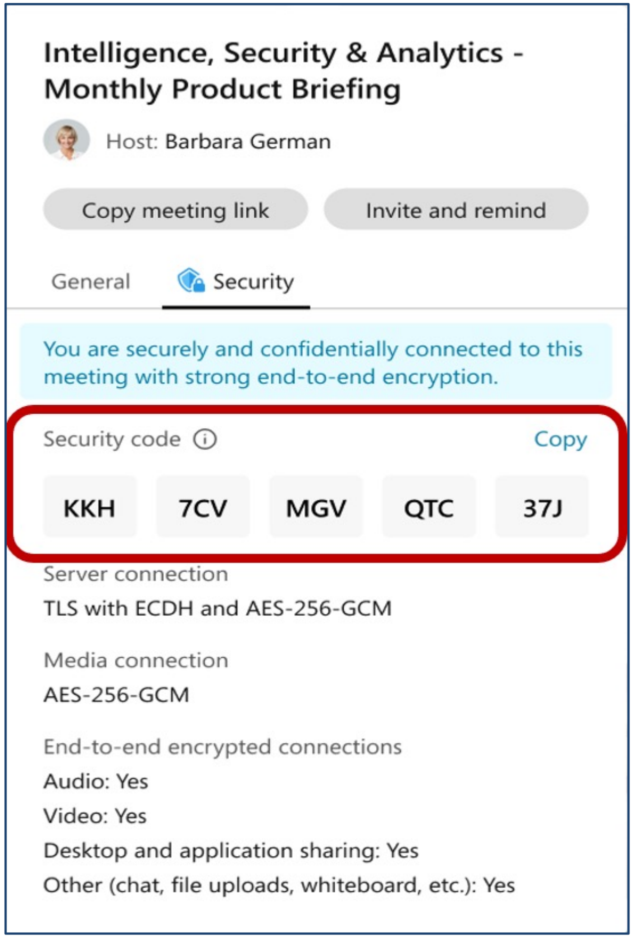
KKH 7CV MGV QTC 37J

Server connection
TLS with ECDH and AES-256-GCM

Media connection
AES-256-GCM

End-to-end encrypted connections
Audio: Yes
Video: Yes
Desktop and application sharing: Yes

Meeting Security Codes – Protecting against MITM attacks



Intelligence, Security & Analytics - Monthly Product Briefing

Host: Barbara German

You are securely and confidentially connected to this meeting with strong end-to-end encryption.

KKH 7CV MGV QTC 37J

Server connection
TLS with ECDH and AES-256-GCM

Media connection
AES-256-GCM

End-to-end encrypted connections
Audio: Yes
Video: Yes
Desktop and application sharing: Yes
Other (chat, file uploads, whiteboard, etc.): Yes

The meeting security code is displayed to all meeting participants. If they all have the same value, then they know they have not been intercepted and impersonated by an attacker (Meddler In The Middle (MITM) attack)

The Webex E2E Encrypted Meeting Security code is derived from all participants' MLS key packages

If participants have the same code, they know they agree on all aspects of the group, including the group's secrets and the current participant list.

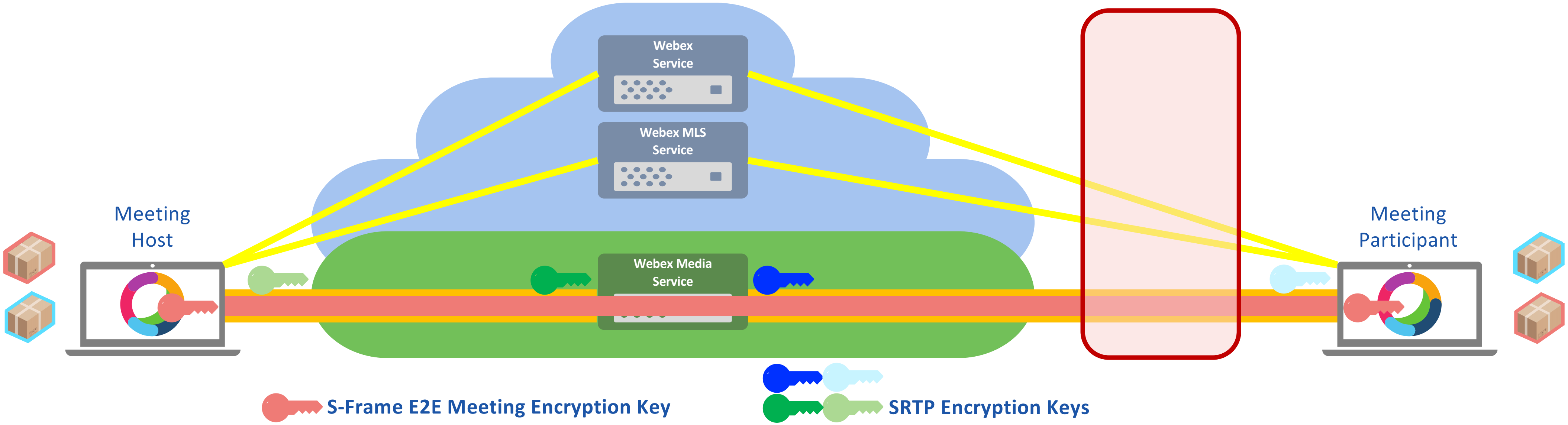
This value changes every time the group key changes, which is at least on every join/leave.

Meeting Security Codes – Protecting against MITM attacks

What a MITM attacker needs to get access to :

Your encrypted media – SRTP encryption keys, all MLS E2E Meeting Encryption keys

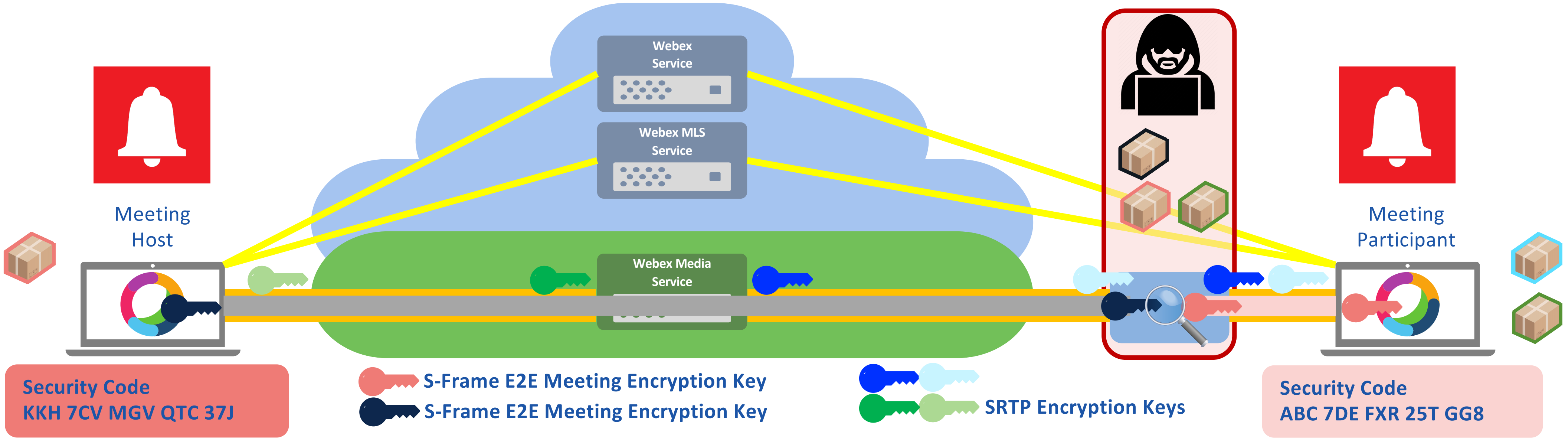
Your TLS connections to Webex, including the MLS service and all MLS key packages



Meeting Security Codes – Protecting against MITM attacks

What a MITM attacker needs access to :
Your encrypted media – SRTP encryption keys, all MLS E2E Meeting Encryption keys
Your TLS connections to Webex, including the MLS service and all MLS key packages

To impersonate you – At a minimum, a MITM attacker needs to :
Intercept all MLS key packages and replace them with their own



Security Code
KKH 7CV MGV QTC 37J

S-Frame E2E Meeting Encryption Key
S-Frame E2E Meeting Encryption Key

SRTP Encryption Keys

Security Code
ABC 7DE FXR 25T GG8

The Security Codes generated by each Webex app using their MLS key packages should match

Zero Trust Security for Webex Meetings

New

End to End Identity

High Level Agenda

End to End Identity

- Q: How do you know that the participants in your meeting are who they say they are ?
- A: You do not rely on your meetings provider to authenticate users, or to provide identity certificates for users or devices
- You authenticate your Users using your Enterprise IdP
- External participants can be authenticated using their Enterprise IdP
- Identity Certificates are generated by a non Cisco CA

Webex Meetings - End to End Identity

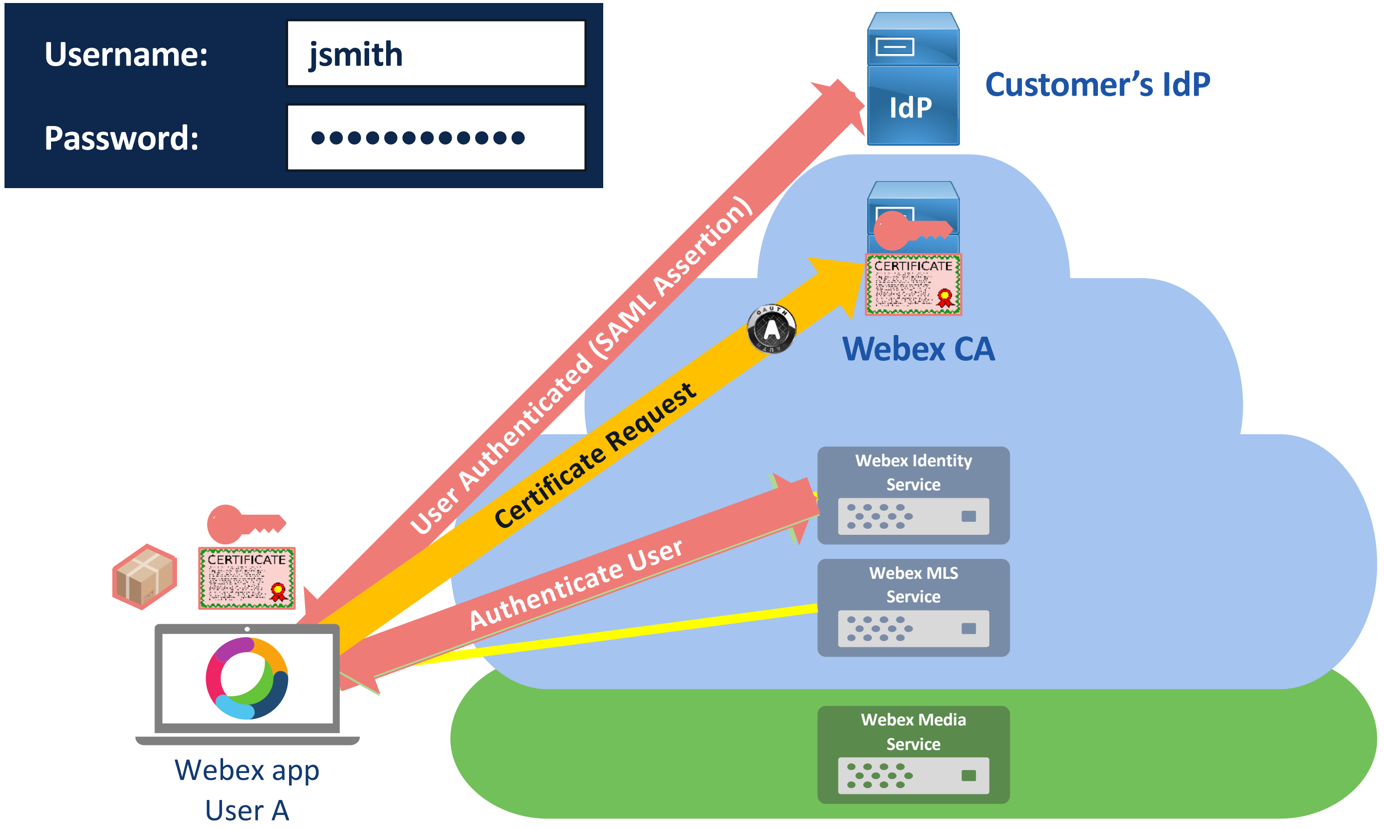
Detailed Agenda

- E2E Encryption - Identity Certificates from Webex CA
- ACME detail
- E2E Identity – Identity Certificates from a non Cisco CA
- Webex Meetings – New User Experience

Review : New Webex E2E Encryption Phase 1

SSO Users authenticating with their Enterprise IdP :

Webex CA Identity certificates



Username: jsmith

Password: ●●●●●●●●●●●●

ACME for E2E Identity with Webex Meetings

Automated Certificate Management Environment (ACME)

The ACME protocol is used to generate user and device identity certificates. ACME automatically handles Certificate Signing Requests sent to Certificate Authorities

Device certificate name validation via public domain name check

User CSR validation via SAML assertion from a federated IdP

https://tools.ietf.org/html/rfc8555
https://tools.ietf.org/html/draft-biggs-acme-sso-00

ACME is protocol that can be used by a Certificate Authority and a Certificate applicant to automate the process of identity verification and certificate issuance…

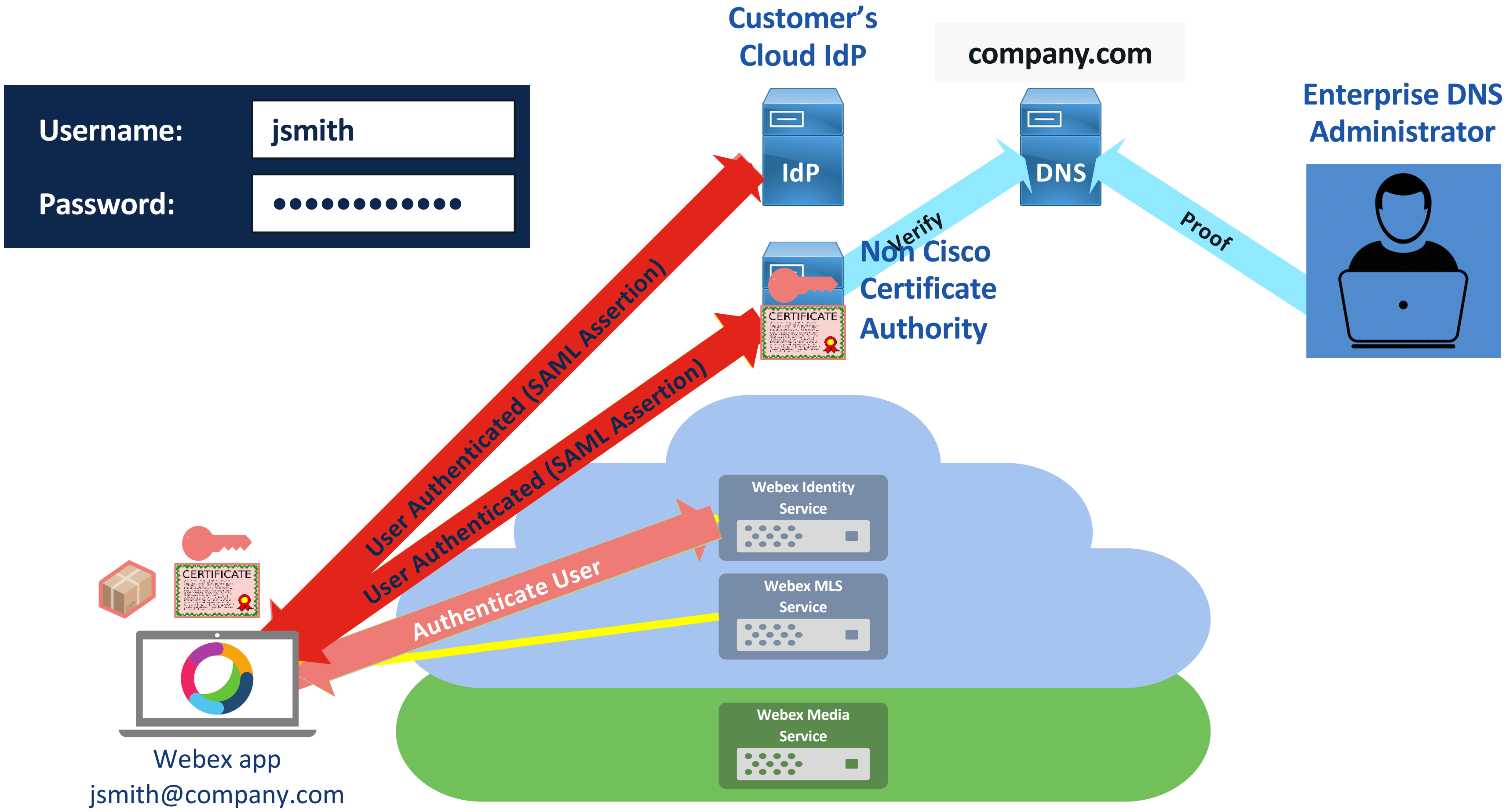
RFC 8555
Describes an automated validation procedure that allows domain-name based certificates (e.g. device1.cisco.com) to be obtained without user intervention.

Draft-biggs-acme-sso
Extends the ACME protocol to enable the ACME service to validate a client's control of an email identifier (e.g. bob@cisco.com) using single sign-on (SSO) technologies

New – Webex End to End Identity Verification

SSO Users authenticating with their Enterprise IdP

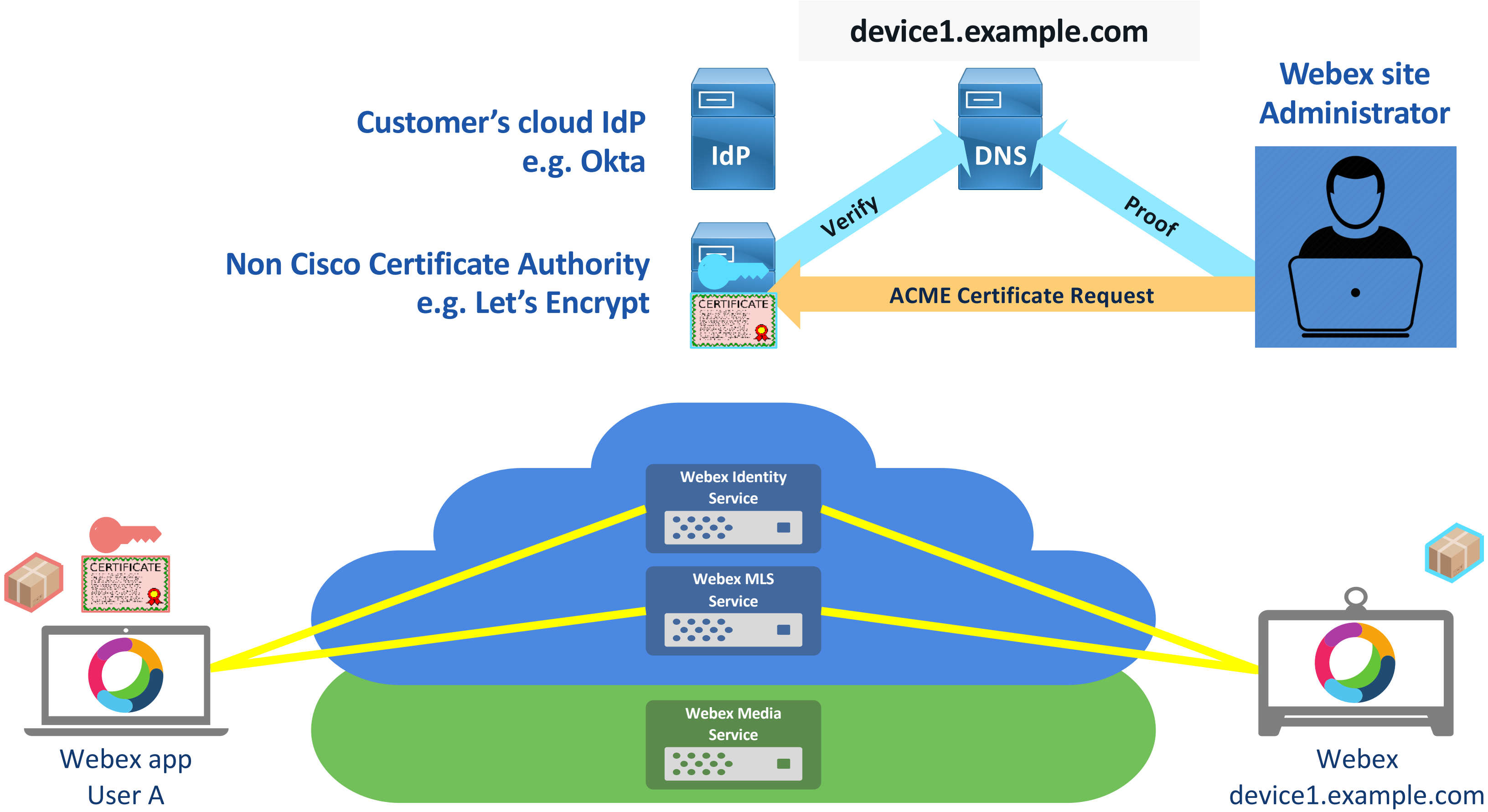
Using ACME to request a signed User Identity certificate from a non Cisco CA



New – Webex End to End Identity Verification

Webex device using ACME to request a signed Certificate from a non Cisco CA

Device Identity

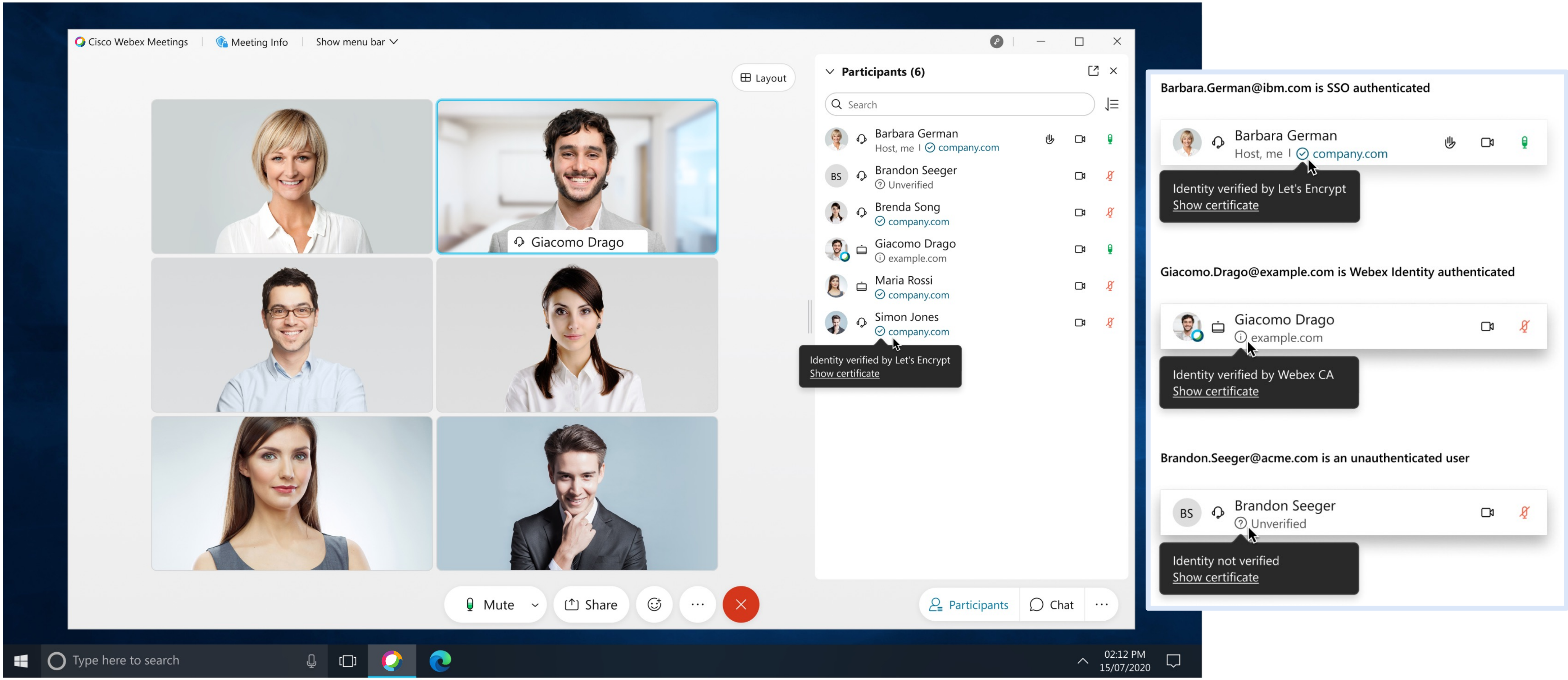


Zero Trust Security for Webex Meetings : Phase 2
Webex E2E Identity

User/Device Authentication and Identity Certificates

User/Device Type	Authentication	Certificate Authority	Lobby/Roster User status
Webex app	Not Signed In / Un-Authenticated (Meeting Join without Sign In)	Webex CA	? **Unverified** (Hover on icon for CA and Cert details)
Webex app	**Webex Identity service or Enterprise IdP (SSO)**	Webex CA	ⓘ example.com (Hover on icon for CA and Cert details)
Webex app	Enterprise IdP (SSO)	Non Cisco CA	✓ example.com (Hover on icon for CA and Cert details)
Webex Cloud registered Device	Machine Account	Webex CA	ⓘ example.com (Hover on icon for CA and Cert details)
Webex Cloud registered Device	Machine Account	Non Cisco CA	✓ example.com (Hover on icon for CA and Cert details)

Zero Trust Security for Webex Meetings : Phase 2
Webex E2E Identity
Meeting Roster - New User Details



Participants (6)

- Barbara German — Host, me | company.com
- Brandon Seeger — Unverified
- Brenda Song — company.com
- Giacomo Drago — example.com
- Maria Rossi — company.com
- Simon Jones — company.com

Identity verified by Let's Encrypt
Show certificate

Barbara.German@ibm.com is SSO authenticated

Barbara German
Host, me | company.com

Identity verified by Let's Encrypt
Show certificate

Giacomo.Drago@example.com is Webex Identity authenticated

Giacomo Drago
example.com

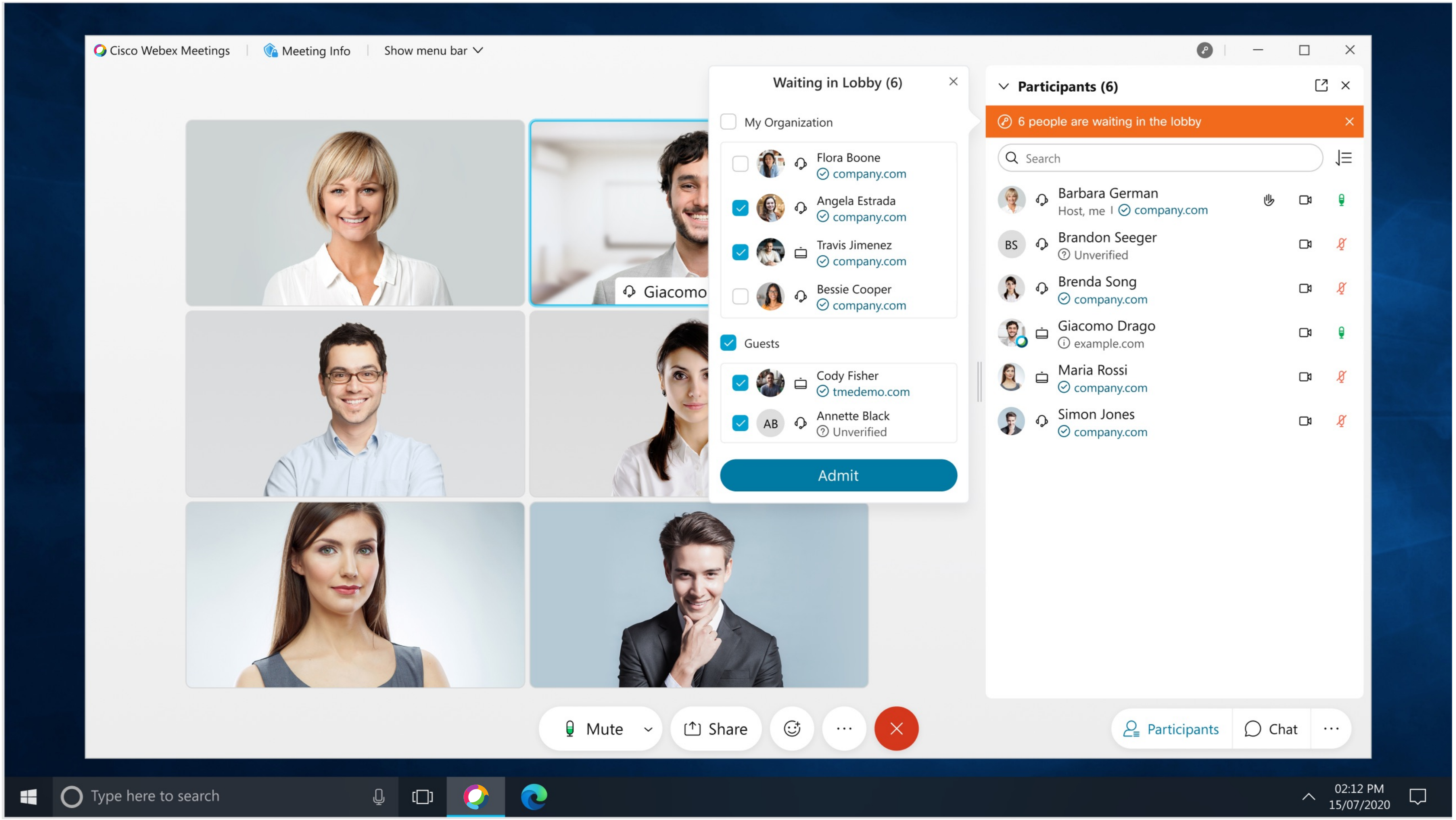
Identity verified by Webex CA
Show certificate

Brandon.Seeger@acme.com is an unauthenticated user

BS Brandon Seeger
Unverified

Identity not verified
Show certificate

Zero Trust Security for Webex Meetings: Phase 2
Webex E2E Identity
Meeting Lobby – New User Details



Cisco Webex Meetings | Meeting Info | Show menu bar

Waiting in Lobby (6)

□ My Organization

- □ Flora Boone ✓ company.com
- ☑ Angela Estrada ✓ company.com
- ☑ Travis Jimenez ✓ company.com
- □ Bessie Cooper ✓ company.com

☑ Guests

- ☑ Cody Fisher ✓ tmedemo.com
- ☑ AB Annette Black ? Unverified

Admit

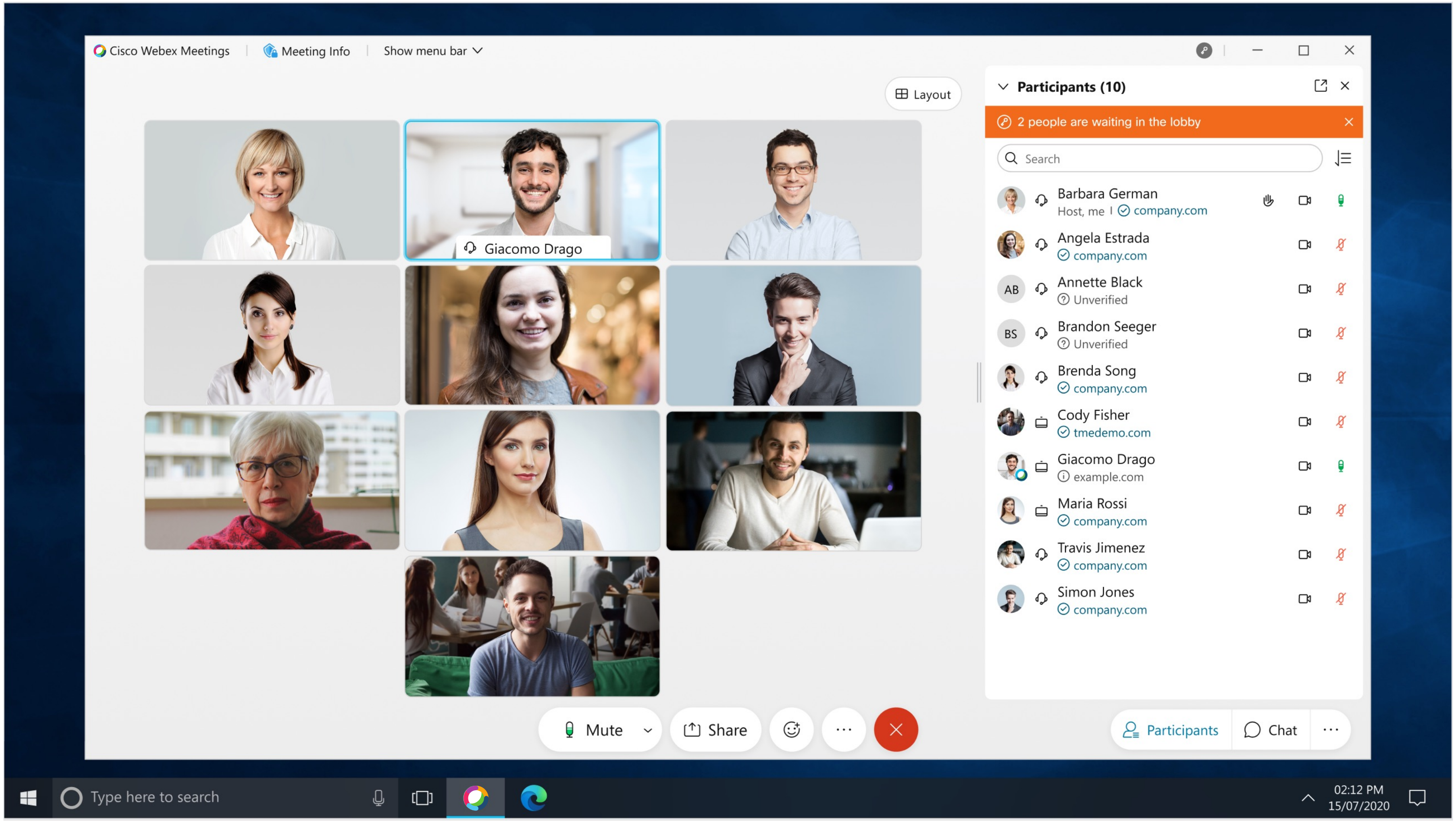
Participants (6)

6 people are waiting in the lobby

Search

- Barbara German — Host, me | ✓ company.com
- BS Brandon Seeger — ? Unverified
- Brenda Song — ✓ company.com
- Giacomo Drago — ⓘ example.com
- Maria Rossi — ✓ company.com
- Simon Jones — ✓ company.com

Zero Trust Security for Webex Meetings: Phase 2
Webex E2E Identity
Meeting Lobby – New User Details



Participants (10)

2 people are waiting in the lobby

Barbara German
Host, me | company.com

Angela Estrada
company.com

Annette Black
Unverified

Brandon Seeger
Unverified

Brenda Song
company.com

Cody Fisher
tmedemo.com

Giacomo Drago
example.com

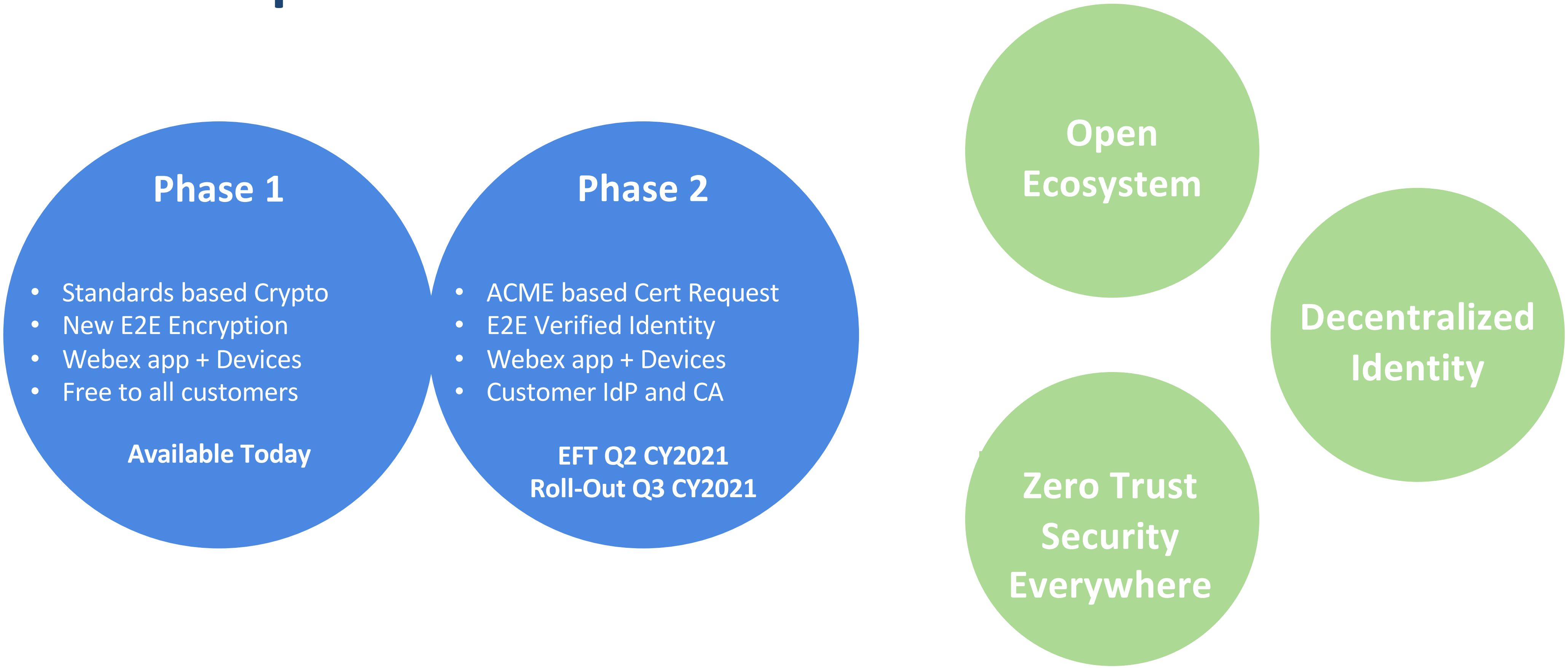
Maria Rossi
company.com

Travis Jimenez
company.com

Simon Jones
company.com

Summary and Roadmap

Zero Trust Security for Webex Meetings Summary and Roadmap



Phase 1

- Standards based Crypto
- New E2E Encryption
- Webex app + Devices
- Free to all customers

Available Today

Phase 2

- ACME based Cert Request
- E2E Verified Identity
- Webex app + Devices
- Customer IdP and CA

EFT Q2 CY2021
Roll-Out Q3 CY2021

Open Ecosystem

Decentralized Identity

Zero Trust Security Everywhere

Zero Trust Security for Webex Meetings

MLS crypto validation and analysis
Code repository – MLS and SFrame

Formal Models and Verified Protocols for Group Messaging:
Attacks and Proofs for IETF MLS
https://hal.inria.fr/hal-02425229/document

Security Analysis and Improvements for the IETF MLS Standard for Group Messaging
https://eprint.iacr.org/2019/1189.pdf

Code Repository – SFrame implementation
https://github.com/cisco/sframe

Code Repository – MLS implementation
https://github.com/cisco/mlspp

Online Documents :

Webex Meetings Security

Security is an integral part of any cloud collaboration sale

- Use this presentation to inform your customers about our new security capabilities for Webex Meetings
- Use existing Webex Security TDM presentations on Sales Connect to educate your customers
- Share existing Webex Security whitepapers with your customers

Webex Meetings Security – Documentation

Zero Trust Security for Webex White Paper
https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html

Webex Meetings Security White Paper
https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html

Webex app – Security White Paper
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Webex-Apps-Security-White-Paper.pdf

Data Handling and Privacy for Cognitive
https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-742369.html

Webex Meetings Privacy Data Sheet
https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf

Network Requirements for Webex Services
https://collaborationhelp.cisco.com/article/WBX000028782

How End to End Encryption works
https://help.webex.com/en-us/WBX44739/What-Does-End-to-End-Encryption-Do

Key Takeaways

- Zero Trust Security =
  Stronger Security for Webex Meetings
- New End to End Encryption for all
- Optional End to End Identity
- End to End Encryption today
- End to End Identity EFT Q2 CY2021
  Roll Out Q3 CY2021

Thank You